TENeT メッセージ仕様書

Ver. 1.0

TEF950-S004-01.00.00/ja

2005 年 3 月
T-Engine フォーラム

目　次

1 はじめに

本仕様書は，TENeT（Trusted Environment with Networking eTRON）仕様 IC カードが備えるべき e^2TP（Extended eTRON Transfer Protocol）メッセージのメッセージセットを規定した仕様書である．

1.1 本仕様書の概要

本仕様書は，権利価値の安全な格納と取引を実現するための，IC カードが備えるべき e^2TP メッセージのメッセージセットである TENeT メッセージを規定する．

TENeT メッセージを搭載した TENeT 仕様 IC カードは，フォルダや権利価値の生成や削除などを実現する基本機能と，アクセス主体の認証や権利価値へのアクセス権限を設定するアクセス制御機能と，権利価値を安全かつ公平に取引する交換機能を有する．

交換機能は，「公平な権利価値取引のための楽観的な交換プロトコル」[THIF03]を採用している．楽観的とは，正常時は 2 者間で交換を完了して，通信の遮断などにより交換が中断して自分の権利価値を紛失した状態や相手の権利価値を未受理の状態となった時に，相手との交換を再開することなく第 3 者機関との間で上記の状態から交換相手と整合する状態に回復すること，である．

TENeT 仕様 IC カードは，これらの機能を有することで，権利価値の安全な格納と IC カード間の権利価値の公平かつ安全な取引を実現する．

1.2 本仕様書の位置付け

TENeT は，権利価値取引を実現する IC カードおよびアプリケーションプログラムの相互運用性を実現するための各種仕様を規定する．仕様の名称と規定する内容を以下に示す．

本仕様書は，TENeT メッセージ仕様を規定する仕様書である．

- TENeT 権利価値取引 API 仕様
  アプリケーションプログラムが IC カードの権利価値を管理・取引するための API
- TENeT メッセージング API 仕様
  アプリケーションプログラムおよび IC カードが e^2 TP メッセージを送受するための API
- Extended eTP （e^2 TP） メッセージ仕様
  e^2 TP メッセージのメッセージフォーマットおよび ISO7816-4 APDU へのマッピング方式
- TENeT メッセージ仕様 【本文書】
  TENeT 仕様 IC カードが備えるべき e^2 TP メッセージのメッセージセット

1.3 規定範囲

本仕様書は，TENeT メッセージとして 2 種類のメッセージセットを規定する．

- 基本メッセージ
  基本機能とアクセス制御機能と，データのバックアップなどの運用機能を実現するメッセージ
- 交換制御メッセージ
  アプリケーションが，IC カードを用いた安全かつ公平な取引を行うための交換機能を実現するメッセージ

1.4 参照規定

- ✓ ISO/IEC Integrated circuit(s) cards with contacts

- Part4: Interindustry commands for interchange, ISO/IEC 7816-4: 1995(E).

✓ 「e²TP メッセージ仕様書」, T-Engine フォーラム , 2005.

1.5 記法

本仕様書で用いる共通の記法を表 2 に定義する.

表 1 記法

記法	意味
a｜b	連接（変数 a と b の連接）
h<x>	メッセージ x を引数とした SHA-1 関数
a := b	変数 a に変数 b を代入
B	バイト
MSB	Most Significant Bit の略. バイト配列の最上位ビットを示す

1.6 登場人物

本仕様書における登場人物は，TENeT 仕様 IC カードである TENeT IC カードと，携帯端末上のアプリケーション(AP)である．TENeT IC カードは，携帯端末に挿入されて，携帯端末のアプリケーション（AP）を用いて利用者から操作される．また権利価値の取引において，取引が中断した場合に，取引中の IC カード間の権利価値の整合性を保証するための調停者である TTP（Trsuted Third Party）が存在する.

TENeT メッセージは，これらの登場人物間で送受されるメッセージである．1.3 節で示した基本メッセージは，AP から IC カードに対する入力メッセージと，IC カードの処理結果を AP へ通知する出力メッセージに種別される．交換制御メッセージは，AP から IC カードに対する入力メッセージと，IC カードから他の IC カードや AP や TTP に送付される出力メッセージに種別される.

1.7 メッセージタイプ

基本／交換メッセージは，e² TP メッセージの DATA 部に入力される．e²TP メッセージは，各 TENeT メッセージを識別するためのメッセージタイプを持つ.

メッセージタイプは上位 1 バイトで基本または交換メッセージを表す大分類，下位 1 バイトで基本または交換メッセージの小分類を表す．TENeT は，上位 1 バイトのうち，00h を基本メッセージ，01h を交換メッセージの値として割り当てる.

本仕様書で規定される TENeT メッセージの下位 1 バイトの小分類を表 3 に示す.たとえば,CreateFile メッセージは，メッセージタイプの上位 1 バイトは 00h，下位 1 バイトは 40h となる.

表 3 基本／交換メッセージのメッセージタイプ下位 1 バイトの小分類

基本小分類	b7	b6	b5	b4	b3	b2	b1	b0	16 進表記
CreateFile	0	1	0	0	0	0	0	0	40h
DeleteFile	0	1	0	0	0	0	0	1	41h
RequestFileInfo	0	1	0	0	0	0	1	0	42h
MoveFile	0	1	0	0	0	0	1	1	43h
RequestFileList	0	1	0	0	0	1	0	0	44h
CreateFolder	0	1	0	0	0	1	0	1	45h
DeleteFolder	0	1	0	0	0	1	1	0	46h
RequestFolderList	0	1	0	0	0	1	1	1	47h
RequestID	0	1	0	0	1	0	0	0	48h
BackUpCard	0	1	0	0	1	0	0	1	49h

RestoreCard	0	1	0	0	1	0	1	0	4Ah
ReformatCard	0	1	0	0	1	0	1	1	4Bh
RequestCardInfo	0	1	0	0	1	1	0	0	4Ch
RequestChallenge	0	1	0	0	1	1	0	1	4Dh
Authenticate	0	1	0	0	1	1	1	0	4Eh
SuccessfulOperation	0	0	1	0	0	0	0	0	20h
SuccessfulFileOperation	0	0	1	0	0	0	0	1	21h
SuccessfulFolderOperation	0	0	1	0	0	0	1	0	22h
FileInfo	0	0	1	0	0	0	1	1	23h
FileList	0	0	1	0	0	1	0	0	24h
FolderList	0	0	1	0	0	1	0	1	25h
DelegatedID	0	0	1	0	0	1	1	0	26h
BackUpInfo	0	0	1	0	0	1	1	1	27h
CardInfo	0	0	1	0	1	0	0	0	28h
Challenge	0	0	1	0	1	0	0	1	29h
AuthMode	0	0	1	0	1	0	1	0	2Ah
UnsuportedMessage	1	0	1	0	0	0	0	0	A0h
AccessViolation	1	0	1	0	0	0	0	1	A1h
ObjectNotFound	1	0	1	0	0	0	1	0	A2h
IllegalParameters	1	0	1	0	0	0	1	1	A3h
MemoryOverflow	1	0	1	0	0	1	0	0	A4h
MaximumNumberExceeded	1	0	1	0	0	1	0	1	A5h
MessageSizeOverflow	1	0	1	0	0	1	1	0	A6h
InternalError	1	0	1	0	0	1	1	1	A7h
(RFU)				(その他の値)					**h

交換小分類	b7	b6	b5	b4	b3	b2	b1	b0	16 進表記
StartExchange	0	1	0	0	0	0	0	0	40h
Offer	0	0	1	0	0	0	0	1	21h
AgreeExchange	0	1	0	0	0	0	1	0	42h
Agreement	0	0	1	0	0	0	1	1	23h
ConfirmExchange	0	1	0	0	0	1	0	0	44h
Confirmation	0	1	1	0	0	1	0	1	65h
Commitment	0	1	1	0	0	1	1	0	66h
RecoverExchange	0	1	0	0	0	1	1	1	47h
ArbitrationRequest	0	0	1	0	1	0	0	0	28h
Arbitration	0	1	0	0	1	0	0	1	49h
RequestExgStatusInfo	0	1	0	0	1	0	1	0	4Ah
CancelExchange	0	1	0	0	1	0	1	1	4Bh
RequestExgStatusList	0	1	0	0	1	1	0	0	4Ch
ExchangeCommitted	0	0	1	0	1	1	0	1	2Dh
ExchangeAborted	0	0	1	0	1	1	1	0	2Eh
ExgStatusInfo	0	0	1	0	1	1	1	1	2Fh
ExgStatusList	0	0	1	1	0	0	0	0	30h
ExchangeSuspended	1	0	1	0	1	0	0	0	A8h
IncompatibleStatus	1	0	1	0	1	0	0	1	A9h

2 データ定義

本章は，TENeT IC カードが利用するデータのフォーマットと値を規定する．

2.1 公開鍵証明書

TENeT IC カードは，eTRON/16 仕様で規定されている 16 バイトの識別子である eTRON ID を IC カードの識別子として利用する．eTRON ID の詳細な仕様は，「e²TP メッセージ仕様書」[TEE2]を参照のこと．

TENeT IC カードが持つ公開鍵証明書を表 4 に示す．公開鍵証明書は，公開鍵証明書発行局（CA: Certificate Authority）により，TENeT IC カードが持つ eTRON ID が正しく発行された eTRON ID であることを保証する．本仕様は，公開鍵証明書の値について，Ver=02h を規定値とする．また TENeT で利用できる署名アルゴリズムの内訳と規定値を表 5 に示す．

表 4　公開鍵証明書

#	記号	サイズ（バイト）	意味	値
1	Ver	1	公開鍵証明書のバージョン	02h
2	CA_ID	16	CA の eTRON ID	
3	Serial_no	4	証明書シリアル番号	
4	Time/Start	4	鍵利用開始日時	
5	Time/End	4	鍵利用終了日時	
6	eTRON ID	16	証明書が証明している eTRON ID	
7	MyKeyVer	1	自公開鍵のバージョン	
8	MyKeyAlgorithm	1	自公開鍵アルゴリズム	表 5 参照
9	MyPublicKey	variable	自公開鍵本体	
10	SignAlgorithm	1	CA 付与の署名アルゴリズム	表 5 参照
11	Sign	variable	CA 付与署名(CA 秘密鍵による#1～#10 の署名値)	

表 5 署名アルゴリズム

#	記号	ビット長	値
1	ECDSA（素体）	160	01h（*1）
4	ECDSA （2 の拡大体）	(RFU)	(RFU)
8	RSA	1024	02h
10	DSA	1024	03h
12	(RFU)	--	-- h

（*1）ECDSA（素体）160 ビットのドメインパラメータを表 5 に示す．

表 6　ドメインパラメータの規定値

項目	値
楕円曲線パラメータ a	07 25 46 B5 43 52 34 A4 22 E0 78 96 75 F4 32 C8 94 35 DE 52 42
楕円曲線パラメータ b	00 C9 51 7D 06 D5 24 0D 3C FF 38 C7 4B 20 B6 CD 4D 6F 9D D4 D9
ベースポイント P.x	07 AF 69 98 95 46 10 3D 79 32 9F CC 3D 74 88 0F 33 BB E8 03 CB
ベースポイント P.y	01 EC 23 21 1B 59 66 AD EA 1D 3F 87 F7 EA 58 48 AE F0 B7 CA 9F
ベースポイント P の位数	04 00 00 00 00 00 00 00 00 00 01 E6 0F C8 82 1C C7 4D AE AF C1
ベースポイント Q.x	06 CE 98 1C B0 D2 7B 4B 3A 71 98 F1 A1 5B 53 6D C2 E6 12 29 95
ベースポイント Q.y	05 0D D9 9B 8F D9 FF 4B 68 F2 80 36 4D 02 49 B7 AF 57 AB 4E 74

2.2 eTRON ID

eTRON ID は,「e²TP メッセージ仕様書」[TEE2]で規定された 16 バイトの識別子である.

TENeT では, eTRON ID のうち, 上位 12 バイトを「domain」, 下位 4 バイトを「port」と呼ぶ. TENeT IC カードは, port=0000h をカード自身が利用する port とするため, TENeT IC カードの eTRON ID は domain|0000h となる. TENeT IC カードは, この eTROn ID を e2TP メッセージの送受時の識別子として用いる.

また TENeT IC カードは AP からの要求に応じて pprt を生成して,「domain|port」を AP の識別子として, AP に払い出す. Port は IC カード内で一意の値である. AP は, この識別子を e²TP メッセージの送受時の識別子として用いる.

3 IC カード機能

本章では，TENeT IC カードが有する機能と TENeT IC カード内のデータ構造，アプリケーションの認証方法など，TENeT IC カードの共通的な特徴を説明する．

3.1 機能概要

TENeT IC カードは，権利価値の生成・削除・閲覧などの権利価値の操作と管理と，権利価値を保護する所有者認証やアクセス制御と，権利価値の IC カード間の安全かつ公平な取引のための機能を提供する．

TENeT IC カードに上記の機能を与える TENeT メッセージ仕様は，基本メッセージと交換制御メッセージから構成される．各メッセージは以下の機能を提供する．メッセージの詳細な動作やパラメータは５章および６章において説明する．

- 基本メッセージ
  - 権利価値やフォルダの生成・削除・閲覧などの基本的なユーザ操作を実現する基本機能と，権利価値へのアクセス権限設定と IC カードへのアクセス主体の認証を行うアクセス制御機能を
  - カード内のデータのバックアップなど実運用のための運用機能
- 交換制御メッセージ
  - TENeT IC カード間で権利価値の安全かつ公平な取引を実現する機能

3.2 IC カードのデータ構造

本節では，TENeT IC カードのデータ構造について説明する．

3.2.1 静的データ／動的データ

TENeT IC カードが記憶・管理するデータとして，静的データと動的データがある．

- 静的データ

  静的データは IC カードの初期化時に不揮発性メモリに書き込まれて，以降の書き換えが発生しないデータである．静的データには，初期設定データなどが該当する．初期設定データを表 7 に示す．
- 動的データ

  動的データは初期化以後も書き換えの発生するデータである．動的データは，IC カードの OS の機能により書き換え時の原子性が保証される．保証されるデータのサイズは IC カードの仕様により異なる．動的データとして，フォルダとファイルが該当する．3.2.3 節以降でフォルダとファイルの構造について説明する．

3.2.2 初期設定データ

TENeT IC カードは初期設定データとして表 7 のデータを不揮発性メモリに記憶する．所有者証明書の内訳は表 4 の通りである．所有者証明書は CA の公開鍵を用いて正当性の検証が可能である．

これらの初期設定データの IC カードへの設定・変更手段については，本仕様では規定しない．

表 7　IC カード初期設定データ

データ	意味
CA の公開鍵	所有者証明書検証用 CA 公開鍵
ECDSA 秘密鍵	IC カードが所有する秘密鍵
所有者パスワード	所有者認証用パスワード
所有者証明書	（eTRON ID の正当性を保証する）公開鍵証明書
LOCK 用パスワード	IC カードへの書き込みの LOCK 用パスワード

3.2.3 フォルダ／ファイル構造

動的データであるフォルダとファイルの特徴は以下の通りである．フォルダとファイルの関係を図 1 に示す．

- フォルダ
  フォルダは 1 階層構造であり，ルートフォルダは存在しない．最大フォルダ数は，それぞれの IC カードの実装に依存する．
- ファイル
  1 ファイルは 1 つの権利価値に相当する．各ファイルはフォルダ内に格納されて管理される．IC カード内の最大ファイルサイズはそれぞれの IC カードの実装に依存する．

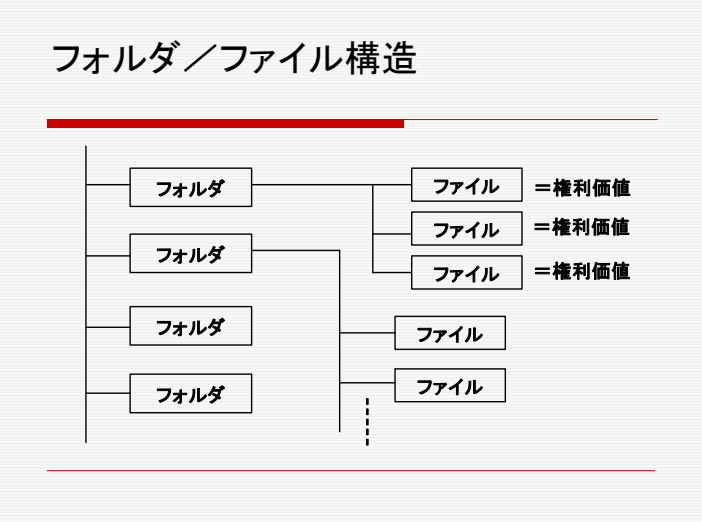

図 1　フォルダ／ファイル構造

3.2.4 フォルダ構造詳細

IC カードは各フォルダについて表 8 のフォルダ情報を持つ．IC カードはカード内のフォルダのフォルダ情報をリスト形式のフォルダリストとして管理する．

表 8 フォルダ情報

データ	意味
Foldername	IC カードの所有者が付与するフォルダ名
folderACL	IC カードの所有者が付与するアクセス権限
folderID	IC カードが割り当てるフォルダ識別子

3.2.5 ファイル構造詳細

IC カードは各ファイルについて表 9 のファイル情報を持つ．また、ファイルは以下の特徴を持つ．

- ✓ 1 つのファイルは 1 種類の権利価値に相当する．
- ✓ 同じ種類の権利価値は 1 つの権利価値にまとめられ，ファイルの個数が加算される．
- ✓ ファイルは生成した IC カードの eTRON ID が付与されるため，偽造されない．
- ✓ ファイルの作成者 ID や内容が，流通過程において変更されることはない．

表 9 ファイル情報

データ	意味
fileID	IC カードが割り当てるファイル識別子
fileCnt	ファイルの個数
fileACL	ファイル生成者が付与するアクセス権限
issuerID	ファイル生成者の eTRON ID
fileLEN	fileDATA のデータサイズ
fileDATA	ファイル生成者が設定するファイルの内容

3.3 フォルダ／ファイルのアクセス権限

TENeT IC カードは，カード内の権利価値を保護するために，フォルダとファイルに対するアクセス権限を設定する．TENeT IC カードは，フォルダとファイルのアクセス権限に従ってアクセス制御を行う．

3.3.1 フォルダアクセス権限

フォルダに設定されるフォルダアクセス権限を表 8 に示す．設定できるのは TENeT IC カードの所有者のみである．たとえば，フォルダアクセス権限が“101”である場合，所有者以外もフォルダ内のファイルの読み込みと譲渡・交換が可能であるが，create はできない．

TENeT IC カードの所有者には，表 10 のフォルダアクセス権は適用されないが，表 9 に示すファイルアクセス権が適用される．

表 10　フォルダアクセス権限

ビット列	意味	概要
100	Read 権許可	フォルダ内のファイルを所有者以外も読み込み可能
010	Create 権許可	フォルダ内のファイルを所有者以外も作成可能
001	Transfer 権許可	フォルダ内のファイルを所有者以外も譲渡・交換可能

3.3.2 ファイルアクセス権限

ファイルに設定されるアクセス権限を表 9 に示す．設定できるのはファイルの生成者のみである．たとえば，ファイルアクセス権限が“01”の場合，所有者以外もファイルの譲渡と交換が可能であるが，コピーはできない．ファイルの生成者がファイルを操作する場合は表 11 のアクセス権は適用されない．

表 11　ファイルアクセス権限

ビット列	意味	概要
10	Copy 権許可	ファイルをファイルの生成者以外もコピー可能
01	Transfer 権許可	ファイルをファイルの生成者以外も譲渡・交換可能

3.4 認証

3.4.1 認証モード

TENeT IC カードは，「非認証モード」と「所有者モード」の 2 種類の認証モードを持つ．メッセージの受信時に認証モードによりそのメッセージの実行許可・不許可を制御する．

TENeT IC カードの初期状態は非認証モードである．TENeT IC カードは，アクセス主体からの認証要求に対して，アクセス主体が指定した認証モードに応じた認証を行う．認証が成功すると IC カードの認証モードは指定された認証モードに遷移する．認証に失敗した場合は，IC カード内の認証モードは遷移しない．

3.4.2 所有者認証

TENeT IC カードは，AP（を操作する利用者）が IC カードの所有者であることを以下の方法により認証する．

まず TENeT IC カードは，AP から RequestChallenge メッセージ（5.2.2 節）を受理してチャレンジを生成して，チャレンジを含む Challenge メッセージ（5.3.2 節）を AP へ送信する．

AP は，Challenge メッセージを受理し，チャレンジを取得すると，チャレンジと 1.9.1 節で示した初期設定データの所有者認証用 PIN の連結した値のハッシュ値 h<チャレンジ|PIN>と所有者モードを示す mode を DATA とする Authenticate（5.2.3 節）メッセージを IC カードへ入力する．

IC カードはチャレンジと PIN が正しく認証できれば，Authenticate メッセージの送信元の AP に所有者モードとしてのアクセス権限を与える．認証に失敗した場合は，元の非認証モードのままである．

IC カードは，Authenticate メッセージの送信元の識別子と遷移後の認証モードを組として，複数の組をリスト形式で管理する．IC カードは，資源の制約のため一定数以上の認証の組を忘れていく．リストに格納される認証状態の組の個数は実装に依存する．上限を超えて新たに認証の組を記憶する場合は LRU（Least Recently Used）でリストに格納された認証状態の組を忘れていく．すなわち，認証状態の組の個数が上限を超えた場合，格納している認証状態の組の中で，最も長い間メッセージのやり取りをしていない送信元に対応する認証状態の組が削除される．

3.4.3 ローカルアクセスとリモートアクセス

TENeT IC カードは，AP や他の TENeT IC カードからのアクセスをローカルアクセスかリモートアクセスかのいずれかで受理する．

ローカルアクセスとは TENeT IC カードが挿入された携帯端末内の AP からのアクセスであり，同端末内の AP のアクセスであるか否かは 2.3 節の AP の識別子により判断する．

すなわち，送信元の識別子の domain が TENeT IC カードの domain と等しい場合は，TENeT IC カードはそのアプリケーションからのアクセスをローカルアクセスとして受理する．逆に他の TENeT IC カードや AP の識別子の domain は TENeT IC カードの domain と異なるため，それらの装置からのアクセスをリモートアクセスとして受理する．

TENeT IC カードは，リモートアクセスで受理したメッセージについてはすべて非認証モードで実行する．

3.4.4 認証モードとメッセージの関係

Authenticate メッセージ（5.2.3 節）による所有者モードでの所有者認証が成功すると，ローカルアクセスは所有者モードでのアクセスとなる．各認証モードと TENeT メッセージの実行許可／不許可の関係を表 10 に示す．

表 10　各メッセージと認証モードとの関係

メッセージ分類	メッセージ名	非認証モード	所有者モード
基本メッセージ	CreateFile	×	○
	DeleteFile	×	○
	RequestFileInfo	※（フォルダの read 権=1）	○
	MoveFile	×	○
	CreateFolder	×	○
	DeleteFolder	×	○
	RequestFileList	※（フォルダの read 権=1）	○
	RequestFolderList	○	○
	RequestID	○	○
	BackUpCard	×	○
	RestoreCard	×	○
	ReformatCard	×	○
	RequestCardInfo	○	○
	RequestChallenge	○	○
	Authenticate	○	○
交換メッセージ	StartExchange	×	○
	AgreeExchange	×	※(ファイル v2 の transfer 権=1)
	ConfirmExchange	×	※(ファイル v1 の transfer 権=1)
	Confirmation	○	○
	Commitment	○	○
	RecoverExchange	×	○
	Arbitration	○	○
	RequestExgStatusInfo	×	○
	RequestExgStatusList	×	○

	CancelExchange	×	○

凡例　○： IC カードがメッセージを受理して処理を実行する
　　×： IC カードが受理せずにエラーとして処理する
　　※： 括弧内の条件が満たされていれば IC カードはメッセージの処理を実行する

3.5 データ領域のバックアップ

TENeT IC カードは，メモリ領域からファイルを格納するために用いるファイル領域を確保する．このファイル領域のサイズは Reformat メッセージ（5.2.14 節）を用いて変更できる．

ファイル領域のサイズの変更時はファイル領域が一旦すべて消去されるため，TENeT IC カード内のデータを携帯端末のメモリに一時的に退避する BavkUp メッセージ（5.2.13 節）を有する．TENeT IC カードは BackUp メッセージを受理すると，退避するカードのデータである backupinfo とカード内で生成した乱数 random とを連結して，署名を付与したデータ（backupinfo|random）PK_{ICC} を含む BackUpInfo メッセージを出力する．random はバックアップが完了するまでカード内に保持する．

TENeT IC カードは，BackUpInfo メッセージを送信すると，LOCKED 状態となって他のメッセージによるバックアップ中のファイル領域へのアクセスを禁止する．

backupinfo の再格納時には，Restore メッセージを用いて AP から IC カードに対して（backupinfo|random）PK_{ICC} を入力する．IC カードは，署名の検証が正しく行われ，random と自身が保持する乱数が正しく照合できると backupinfo を再度ファイル領域に格納してバックアップを完了する．

4 IC カードのメッセージ処理

4.1 メッセージタイプによる処理の分岐

TENeT IC カードは，受理した TENeT メッセージをメッセージタイプにより識別する．

IC カードは, 1.8 節の表 3 に規定されていないメッセージタイプであった場合は UnsupportedMessage メッセージを返却する．

また，e²TP メッセージの DATA である TENeT メッセージのサイズを示す LEN 値と，実際の DATA のサイズが異なる場合は，IllegalParameters メッセージを出力する．

4.2 各メッセージの処理

4.1 節のエラーメッセージを返却しない場合は，表 3 に規定されたメッセージタイプに基づいて，5 章以降の各メッセージに定められた処理を行う．各メッセージの項目について説明する．

4.2.1 Parameters

TENeT メッセージの各値である．メッセージの値はメモリ領域に上から順番に配置される．

4.2.2 Output

入力された TENeT メッセージが正常に処理された場合に, IC カードが出力する TENeT メッセージである．

4.2.3 Exceptional Output

入力された TENeT メッセージの処理が異常終了した場合に出力される TENeT メッセージである．Exceptional Output で出力される TENeT メッセージはエラーの発生原因により異なる．

5 基本メッセージ

5.1 登場人物

基本メッセージの登場人物は，TENeT IC カードと，TENeT IC カードを操作する携帯端末上のアプリケーション（AP）である．基本メッセージは，AP から TENeT IC カードへの操作命令である入力メッセージと，入力メッセージに対する処理結果として TENeT IC カードから AP に送付される出力メッセージに分類される．

本仕様書では，4.2 節で AP から TENeT IC カードへの入力メッセージを，4.3 節で TENeT IC カードから AP への出力メッセージを規定する．

5.2 アプリケーションから IC カードへの入力メッセージ

5.2.1 RequestID

AP が IC カードに対して ID の払い出しを要求するメッセージ．

AP が本メッセージの生成時に指定する DATA は空である．

メッセージを受理した IC カードは，送信元の識別子と組である認証状態に関係なく，port を生成して IC カードの domain と連結した識別子 AP_ID （domain|port）を生成する．

IC カードは，上記処理の正常終了時に，送信元の AP に AP_ID を値とする DelegatedID メッセージを送信する．

IC カードは，上記処理の異常終了時に，送信元の AP に以下のメッセージを送信する．

－ LEN と DATA のサイズが異なる場合は IllegalParameters メッセージを送信する．

－ すべての port が使用済みの場合は MaximumNumberExceeded メッセージを送信する．

Parameters：

DATA 詳細

なし	

Output：

DelegatedID

DATA 詳細

AP_ID	払い出した AP_ID	16B

Exceptional Output：

(エラーメッセージ)	(原因)
IllegalParameters	－ LEN が DATA のサイズと異なる
MaximumNumberExceeded	－ port に空きが無い（すべての port が使用済み）

5.2.2 RequestChallenge

AP が IC カードに対してチャレンジの出力を要求するメッセージ.
AP が本メッセージの入力時に指定する DATA は空である.
メッセージを受理した IC カードは，送信元の AP の domain と IC カードの eTRON ID の domain が等しい時のみ challengedata を生成する.

IC カードは，上記処理の正常終了時に，送信元の AP に challengedata を値とする Challenge メッセージを送信する.
IC カードは，上記処理の異常終了時に，送信元の AP に以下のメッセージを送信する.
- LEN と DATA のサイズが異なる場合は IllegalParameters メッセージを送信する.
- 送信元の AP の domain と IC カードの eTRON ID の domain が異なる場合は，AccessViolation メッセージを送信する.

Parameters :

DATA 詳細

なし

Output :

Challenge

DATA 詳細

challengedata	チャレンジ	20B

Exceptional Output :

(エラーメッセージ)	(原因)
AccessViolation	－ IC カードが LOCKED 状態である／ メッセージの送信元がローカルアクセスではない
IllegalParameters	－ LEN が DATA のサイズと異なる

5.2.3 Authenticate

AP が IC カードに対して認証を指示するメッセージ.

AP は本メッセージを送信する前に, RequestChallenge メッセージにより challengedata を取得している必要がある.

AP は本メッセージの生成時に,

－所有者モードの場合は, 認証モード mode (=0002h) と保持している challengedata と秘密情報 (IC カードに設定された所有者認証用 PIN) を含む認証情報を指定する.

－非認証モードの場合は, 認証モード mode (=0000h) を指定する.

メッセージを受理した IC カードは, 送信元の domain が IC カードの eTRON ID の domain と等しい時のみ認証を行う (認証の方法は 3.4.2 節を参照のこと). TENeT IC カードは認証が成功すると, 指定された認証モードに遷移する. また認証に失敗した場合は指定された認証モードに遷移しない.

IC カードは, 上記処理の正常終了時に, 送信元の AP に遷移後の認証モード mode を含む Authmode メッセージを送信する.

IC カードは, 上記処理の異常終了時に, 送信元の AP に以下のメッセージを送信する.

－LEN と DATA のサイズが異なる場合は IllegalParameters メッセージを送信する.

―送信元の domain と IC カードの eTRON ID の domain が異なる場合は, AccessViolation メッセージを送信する.

－mode 値が 0000h か 0002h でない場合は, IllegalParameters メッセージを送信する.

Parameters :

DATA 詳細

所有者モードの場合

mode	認証モード	2B
Authenticator	認証用情報	20B
	IC カードから取得した challengedata (ch) と秘密情報 (pw) のハッシュ値 h (ch | pw)	

非認証モードの場合

mode	認証モード	2B
	所有者モードを指定 : mode=0002h	
	非認証モードを指定 : mode=0000h	

Output :

AuthMode

DATA 詳細

mode	遷移した結果の認証モード	2B
	所有者モードに遷移 : mode=0002h	
	非認証モードに遷移 : mode=0000h	

Exceptional Output :

(エラーメッセージ)	(原因)
AccessViolation	－ IC カードが LOCKED 状態である／ メッセージの送信元がローカルアクセスではない
IllegalParameters	－ LEN が DATA のサイズと異なる／ mode が 0000h, または 0002h ではない

5.2.4 CreateFile

APがICカードに対してファイルの生成を指示するメッセージ.

AP は本メッセージの生成時に，ファイルの情報であるファイルの内容 fileDATA とファイルサイズ fileLEN とファイルの個数 fileCnt とファイルのアクセス権 fileACL と，ファイル格納先のフォルダ識別子 folderID を指定する.

メッセージを受理した IC カードは，送信元の識別子と組である認証状態が所有者モードであれば，指定されたフォルダにファイルを生成して，ファイル識別子である CreatedID を付与する.

生成されたファイルには，3.2.2 節の所有者証明書内の eTRON ID が付与される．ファイルはこの eTRON ID と組で管理される.

ICカードは，上記処理の正常終了時に，送信元のAPに，生成したファイルの個数createdCntと上記のcreatedIDを含むSucessfulFileOperationメッセージを送信する.

ICカードは，上記処理の異常終了時に，送信元のAPに以下のメッセージを送信する.

－LENとDATAのサイズが異なる場合はIllegalParameterメッセージを送信する.

－送信元を所有者として認証していない場合は，AccessViolationメッセージを送信する.

－folderIDで示されるフォルダが存在しない場合は，ObjectNotFoundメッセージを送信する.

－fileCntが0である場合は，Illegalparameterメッセージを送信する.

－LEN値が最大格納ファイルサイズを超える場合や新たにファイルを作成するための空き容量が無い場合はMemoryOverflowメッセージを送信する.

－加算後のファイル個数がFFFFFFFFhを超える場合はmaximunNemberExceededを送信する.

Parameters：

DATA 詳細

folderID	ファイル格納先のフォルダ識別子	2B
fileCnt	ファイルの個数	4B
fileACL	ファイルのアクセス権	1B
fileLEN	ファイル長	2B
fileDATA	ファイルの内容	(filelen) B

OutPut：

SucessfulFileOperation

DATA 詳細

MessageType	CreateFile の MessageType	2B
createdID	作成したファイルの識別子	2B
createdCnt	作成したファイルの個数	4B

Exceptional OutPut：

（エラーメッセージ）		（原因）
AccessViolaion	－	IC カードが LOCKED 状態である／ 送信元に対応する認証状態が所有者モードでない
ObjectNotFound	－	folderID で示されるフォルダが存在しない
IllegalParamets	－	fileCnt に 0 を入力する
MemoryOverflow	－	LEN が最大格納ファイルサイズを超える／ カードの空き容量がない
MaximumNumberExceed	－	加算後のファイルの fileCnt が FFFFFFFFh を超える

5.2.5 DeleteFile

AP が IC カードに対してファイルの削除を指示するメッセージ.
AP は本メッセージの入力時に，削除するファイルの格納先のフォルダ識別子 folderID と削除するファイルの識別子 fileID と削除するファイル個数 fileCnt を指定する.
メッセージを受理した IC カードは送信元の識別子と組である認証状態が所有者モードであれば，指定されたファイルを削除する.

IC カードは，上記処理の正常終了時に，送信元に，削除したファイルの識別子 deletedID と削除した個数 deletedCnt を含む SucessfulFileOperation メッセージを出力する.
また IC カードは，上記処理の異常終了時に，送信元に以下のメッセージを送信する.
－LEN と DATA のサイズが異なる場合は IllegalParameters メッセージを送信する.
－送信元の識別子と組である認証状態が所有者モードでない場合は，AccessViolation メッセージを送信する.
－folderID で示されるフォルダが存在しない場合は，ObjectNotFound メッセージを送信する.
－delfileCnt が 0 である場合は，IllegalParameters メッセージを送信する.
－メッセージ受理時のファイル個数が delfileCnt より少ない場合は, MaximumNumberExceed メッセージを送信する.

Parameters：

DATA 詳細

folderID	削除するファイルの格納先のフォルダ識別子	2B
fileID	削除するファイルの識別子	2B
fileCnt	削除するファイル個数	4B

Output：

SucessfulFileOperation

DATA 詳細

MessageType	DeleteFile の MessageType	2B
deletedID	削除したファイルの識別子	2B
deletedCnt	削除したファイルの個数	4B

Exceptional Output：

（エラーメッセージ）		（原因）
AccessViolaion	－	IC カードが LOCKED 状態である／ 送信元に対応する認証状態が所有者モードでない
ObjectNotFound	－	folderID で示されるフォルダが存在しない
IllegalParamets	－	LEN が DATA のサイズと異なる／ fileCnt に 0 を入力する
MaximumNumberExceed	－	現在のファイル個数が delfileCnt より少ない

5.2.6 MoveFile

APがICカードに対してフォルダ間のファイルの移動を指示するメッセージ.
APは本メッセージの生成時に，移動するファイルの識別子fileIDと，移動するファイル個数fileCntと，格納元のフォルダ識別子folderIDと，格納先のフォルダ識別子dstfolderIDと，移動とコピーを区別するcopyflagを指定する.
メッセージを受理したICカードは，送信元の識別子と組である認証状態が所有者モードであれば，ファイルを移動する.
ICカードは，格納先のフォルダにファイルの生成者のeTRON IDであるissuerIDとアクセス権fileACLとファイルの内容fileDATAが一致するファイルが存在する場合，fileCnt分を当該ファイルに加算する.
ICカードは,fileCntがファイルの個数と同じ場合,格納元のフォルダからファイルを完全に削除する.copyflagが0でない場合はファイルのコピーとなり，移動元のファイルの個数が減算されない.

ICカードは,上記処理の正常終了時に,送信元のAPにSucessfulFileOperationメッセージを送信する.
ICカードは，上記処理の異常終了時に，送信元に以下のメッセージを送信する.
－LENとDATAのサイズが異なる場合はIllegalParameterメッセージを送信する.
－送信元を所有者として認証していない場合とcopyflag≠00hの時にファイルのコピーが認められていない場合は，AccessViolationメッセージを送信する.
－folderIDで示されるフォルダやfileIDで指定されるファイルが存在しない場合と，移動する個数がファイルの個数を超える場合はは，ObjectNotFoundメッセージを送信する.
－fileCntに0が入力された場合とfolderIDと移動先のdstfolderIDが同じである場合はIllegalparameterメッセージを送信する.
－fileIDで指定されたファイル長が格納可能最大ファイル長を超える場合とコピーする時に空き容量がない場合はMemoryOverflowメッセージを送信する.
－移動先のファイルの個数がFFFFFFFFhを超える場合は，MaximumNumberExceedsを送信する.

Parameters：

DATA詳細

folderID	移動元のファイルの格納先のフォルダ識別子	2B
copyFlag	移動／コピーの指定（=00h：移動／≠00h:コピー）	1B
fileID	移動元のファイルの識別子	2B
fileCnt	移動する個数	4B
dstfolderID	移動先フォルダのフォルダ識別子	2B

Output：

SuccessfulFileOperation

DATA詳細

MessageType	MoveFileのMessageType	2B
fileID	移動先のファイルの識別子ID	2B
fileCnt	移動先の現在のファイルの個数	4B

Exceptional Output：

（エラーメッセージ）		（原因）
AccessViolaion	－	ICカードがLOCKED状態である／ 送信元に対応する認証状態が所有者モードでない／ copyflag≠00hにおいてファイルのcopy権が認められていない
ObjectNotFound	－	folderIDで示されるフォルダやfileIDで示されるファイルが存在しない
IllegalParamets	－	LENがDATAのサイズと異なる／

		folderID と dstfolderID が同じである／ fileCnt に 0 を入力する
MemoryOverflow	－	fileID で指定されたファイルの長さが格納可能最大ファイル長を超える／ カードの空き容量がない
MaximumNumberExceeds	－	移動先のファイルの個数が FFFFFFFFh を超える

5.2.7 RequestFileInfo

APがICカードに対してファイルの読み込みを指示するメッセージ.
APは本メッセージの入力時に，読み込むファイル識別子fileIDと，ファイルが格納されているフォルダ識別子folderIDと，読み込み開始アドレスstartと，読む込み長さlenを指定する.
メッセージを受理したICカードは，送信元の識別子と組である認証状態が所有者モードである時，または認証状態が非認証モードかつフォルダのread権限を許可されている時はファイル情報を送信する.

ICカードは，上記処理の正常終了時に，送信元のAPにファイル情報を含むFileInfoメッセージを送信する.
ICカードは，上記処理の異常終了時に，以下のメッセージを送信する.
－LENとDATAのサイズが異なる場合はIllegalParameterメッセージを送信する.
－送信元の識別子と組である認証状態が所有者モードない場合と，フォルダのread権が許可されていない場合は，AccessViolationメッセージを送信する.
－入力時に指定されたフォルダやファイルが存在しない場合は,ObjectNotFoundメッセージを送信する.

Parameters：

DATA詳細

folderID	読み込むファイルの格納先のフォルダ識別子	2B
fileID	読む込むファイルの識別子	2B
start	読み込み開始アドレス （ファイルのデータの先頭からのOffset値）	2B
len	読み込む長さ	2B

Output：

FileInfo

DATA詳細

filelen	ファイルのデータ長 （実際のファイルのデータ長）	2B
fileCnt	ファイルの個数	4B
fileACL	ファイルのアクセス権	1B
issuerID	ファイルの生成者のeTRON ID	16B
readLen	fileDATAのサイズ （読み出したファイルのデータ長）	2B
fileDATA	ファイルの内容	(readLen) B

Exceptional Output：

（エラーメッセージ）		（原因）
AccessViolaion	－	ICカードがLOCKED状態である／ 送信元に対応する認証状態が所有者モードでない／ フォルダのread権が認められていない
ObjectNotFound	－	folderIDで示されるフォルダやfileIDで示されるファイルが存在しない
IllegalParamets	－	LENがDATAのサイズと異なる

5.2.8 RequestFileList

AP が IC カードに対してファイルリストの出力を指示するメッセージ.
AP は本メッセージの生成時に，ファイルリストを取得するフォルダ識別子 folderID と読み込み開始アドレス start と読み込む長さ len を指定する.
メッセージを受理した IC カードは，送信元の識別子と組である認証状態が所有者モードであれば，または認証状態が非認証モードかつフォルダの read 権が許可されていない場合はファイルリストを出力する.

IC カードは，上記処理の正常終了時に，送信元にファイルリストを含む FileList メッセージを送信する.
IC カードは，上記処理の異常終了時に，送信元に以下のメッセージを送信する.
- LEN と DATA のサイズが異なる場合は IllegalParameters メッセージを送信する.
- 送信元の識別子と組である認証状態が所有者モードでない場合，かつフォルダの read 権が許可されていない場合は，AccessViolation メッセージを送信する.
- フォルダが存在しない場合は，ObjectNotFound メッセージを送信する.
- 読み込むファイルリストのサイズが送信可能最大サイズを超える場合は MessageSizeOverflow メッセージを送信する.

Parameters :

DATA 詳細

folderID	ファイルリストを取得するフォルダの識別子	2B
start	読み込み開始アドレス （ファイルのデータの先頭からの Offset 値）	2B
len	読み込む長さ	2B

Output :

FileList

DATA 詳細

filenum	ファイルリストが管理するファイル個数	2B
fileinfo	ファイルのリスト	filenum*(27+readlen) B

fileinfo 詳細

fileID	ファイル ID	2B
filelen	実際のファイルサイズ	2B
filecnt	ファイル個数	2B
fileACL	ファイル ACL	1B
issuerID	ファイルの発行者 ID	16B
readlen	読み出したファイルデータの長さ	2B
fileDATA	読み出したファイルデータ	(readlen) B

Exceptional Output :

（エラーメッセージ）		（原因）
AccessViolaion	－	IC カードが LOCKED 状態である／ 送信元に対応する認証状態が所有者モードでない／ フォルダの read 権が認められていない
ObjectNotFound	－	folderID で指定されたフォルダが存在しない
IllegalParamets	－	LEN が DATA のサイズと異なる
MessageSizeOverflow	－	ファイルリストのサイズが送信可能最大サイズを超える

5.2.9 CreateFolder

APがICカードに対してフォルダの生成を指示するメッセージ.
APは本メッセージの生成時に，作成するフォルダ名 foldernameと，フォルダのアクセス権 folderACLを指定する.
メッセージを受理した IC カードは，送信元の識別子と組である認証状態が所有者モードであれば，フォルダを生成し，識別子 CeatedfolderID を付与する.

ICカードは，上記処理の正常終了時に，CreatedfolderIDを含むSuccessfulFolderOperationメッセージを送信する.
ICカードは，上記処理の異常終了時に，以下のメッセージを送信する.
－LENとDATAのサイズが異なる場合はIllegalParametersメッセージを送信する.
－送信元の識別子と組である認証状態が所有者モードでない場合は，AccessViolationメッセージを送信する.
－生成するフォルダ名と同一のフォルダが既に存在する場合は，IllegalParametersメッセージを送信する.
－カードにフォルダを生成する空き容量が無い場合はMemoryOverflowメッセージを送信する.

Parameters：

DATA 詳細

foldername	作成するフォルダ名	16B
folderACL	フォルダのアクセス権	1B

Output：

SuccessfulFolderOperation

DATA 詳細

MessageType	CreateFolder メッセージの MessageType	2B
CreatedfolderID	作成したフォルダの識別子	2B

Exceptional Output：

(エラーメッセージ)		(原因)
AccessViolaion	－	IC カードが LOCKED 状態である／ 送信元に対応する認証状態が所有者モードでない
IllegalParamets	－	LEN が DATA のサイズと異なる／ 同一名のフォルダが存在する
MemoryOverflow	－	カードの空き容量がない

5.2.10 DeleteFolder

AP が IC カードに対してフォルダの削除を指示するメッセージ.

AP は本メッセージの生成時に，削除するフォルダの識別子 folderID と，ファイルの削除モード mode を指定する．mode=00h の時はフォルダ内にファイルが存在するとフォルダを削除できない（異常終了）．mode=01h の時はフォルダ内のファイルごと削除する.

メッセージを受理した IC カードは，送信元の識別子と組である認証状態が所有者モードであれば，ファイルを削除する.

IC カードは，上記処理の正常終了時に，送信元の AP に削除したファイルの識別子 deletedfolderID を含む SuccessfulFolderOperation メッセージを送信する.

IC カードは，上記処理の異常終了時に，以下のメッセージを送信する.

－LEN と DATA のサイズが異なる場合は IllegalParameters メッセージを送信する.

－送信元を所有者として認証していない場合と mode=00h を指定した時にフォルダ内にファイルが存在する場合とファイルが交換中である場合は，AccessViolation メッセージを送信する.

－Folderid で示されるフォルダが存在しない場合は ObjectNotFound メッセージを送信する.

－Mode が 00h または 01h でない場合は IllegalParameters メッセージを送信する.

Parameters：

DATA 詳細

folderID	削除するフォルダのフォルダ識別子	2B
mode	フォルダの削除モード	1B
	- mode=00h：フォルダにファイルが存在する場合は異常終了する	
	- mode=01h：ファイルが存在する場合，ファイルごと削除する	

Output：

SuccessfulFolderOperation

DATA 詳細

MessageType	DeleteFolder メッセージの MessageType	2B
deletedfolderID	削除したフォルダ識別子	2B

Exceptional Output：

AccessViolaion	－ IC カードが LOCKED 状態である／ 送信元に対応する認証状態が所有者モードでない／ mode=00h の時にフォルダ内にファイルが存在する／ ファイルが交換中である
ObjectNotFound	－ folderID で示されるフォルダが存在しない
IllegalParamets	－ LEN が DATA のサイズと異なる／ mode が 00h，または 01h ではない

5.2.11 RequestFolderList

AP が IC カードに対してフォルダリストの出力を指示するメッセージ.
AP が本メッセージの生成時に指定する DATA は空である.
メッセージを受理した IC カードは，送信元の識別子と組である認証状態に依存せずにカード内のフォルダリストを取得する.

IC カードは，上記処理の正常終了時に，送信元にフォルダリストを含む FolderList メッセージを送信する.
IC カードは，上記処理の異常終了時に，送信元に以下のメッセージを送信する.
－LEN と実際の DATA のサイズが異なる場合は IllegalParameters メッセージを送信する.

Parameters :

DATA 詳細

なし

Output :

FolderList

DATA 詳細

foldernum	フォルダの個数	2B
folderinfo	フォルダリスト	(foldernum*19)B

folderinfo 詳細

folderID	フォルダ識別子	2B
foldername	フォルダ名	16B
folderACL	フォルダ ACL	1B

Exceptional Output :

AccessViolaion	－	IC カードが LOCKED 状態である
IllegalParamets	－	LEN が DATA のサイズと異なる

5.2.12 RequestCardInfo

AP が IC カードに対して IC カード情報の出力を指示するメッセージ.
AP が本メッセージの生成時に指定する DATA は空である.
メッセージを受理した IC カードは，送信元の識別子と組である認証状態に依存せずにカード情報を取得する.
IC カードは，上記処理の正常終了時に，送信元に対してカード情報を含む CardInfo メッセージを送信する.
IC カードは，上記処理の異常終了時に，以下のメッセージを送信する.
－LEN と実際の DATA のサイズが異なる場合は IllegalParameters メッセージを送信する.

Parameters：

DATA 詳細

なし

Output：

CardInfo

DATA 詳細

ICCState	ICC の状態	1B
SignAlgorithm	ICC が使用可能な署名のアルゴリズム	1B
KeyAlgorithm	ICC が使用可能な鍵のアルゴリズム	1B
Certlen	ICC の公開鍵証明書長	2B
Cert	ICC の公開鍵証明書	(Certlen) B
MaxFolderNum	生成可能最大フォルダ数	2B
MaxFileNum	生成可能最大ファイル数	2B
MaxFileSize	生成可能最大ファイルサイズ	2B
AuthMode	RequestCardInfo の Src の現在の認証モード	2B

Exceptional Output：

(エラーメッセージ)	(原因)
IllegalParameters	－ LEN が DATA のサイズと異なる

5.2.13 BackUpCard

APがICカードに対して保存ファイル情報の出力を指示するメッセージ.
APが本メッセージの入力時に指定するDATAは空である.
メッセージを受理したICカードは，送信元の識別子と組である認証状態が所有者モードであれば保存ファイル情報を取得して，乱数 random を生成し．保存するファイル情報と乱数を連結した値であるbackupinfoを生成して，署名signを付与する．ICカードは3.5節のバックアップが完了するまでrandomを記憶しておく.

ICカードは，上記処理の正常終了時に，送信元にbackupinfoとsignを含むBackUpInfoメッセージを送信する.
ICカードは，上記処理の異常終了時に，以下のメッセージを送信する.
－LENと実際のDATAのサイズが異なる場合はIllegalParametersメッセージを送信する.
－送信元が所有者モードでない場合と交換中のファイルが存在する場合は，AccessViolationメッセージを送信する.
－保存ファイル情報のサイズが送信可能最大サイズを超える場合はMaximumSizeOverflowメッセージを送信する.

Parameters：

DATA詳細

なし

Output：

BackUpInfo

DATA詳細

backupinfolen	保存ファイル情報長＋乱数長	2B
signlen	署名長	2B
backupinfo	保存ファイル情報｜random	(backupinfolen) B
sign	ICカードによるbackupinfoへの署名	(signlen) B

Exceptional Output：

AccessViolation	－	ICカードがLOCKED状態である／ 送信元に対応する認証状態が所有者モードでない／ ファイル交換中である
IllegalParameters	－	LENがDATAのサイズと異なる
MaximumSizeOverflow	－	保存ファイル情報のサイズが送信可能最大サイズを超える

5.2.14 ReformatCard

AP が IC カードに対してファイル領域のリサイズを指示するメッセージ.
AP は本メッセージの生成時にリサイズするサイズである fileSize を指定する.
メッセージを受理した IC カードは，送信元の識別子と組である認証状態が所有者モードであれば，ファイル領域のリサイズを行う.

IC カードは，上記処理の正常終了時に，送信元の AP に SuccessfulOperation メッセージを送信する.
IC カードは，上記処理の異常終了時に，以下のメッセージを送信する.
－LEN と実際の DATA のサイズが異なる場合は IllegalParameters メッセージを送信する.
－送信元の識別子と組である認証状態が所有者モードでない場合は，AccessViolation メッセージを送信する.
－fileSize に 0 を入力した場合と fileSize がバッファ領域サイズを超える場合は，MemoryOverflow メッセージを送信する.

Parameters：

DATA 詳細

fileSize	リサイズするサイズ	2B

Output：

SuccessfulOperation

DATA 詳細

MessageType	ReformatCard メッセージの MessageType	2B

Exceptional Output：

（エラーメッセージ）		（原因）
AccessViolation	－	IC カードが LOCKED 状態である／ 送信元に対応する認証状態が所有者モードでない
IllegalParameters	－	LEN が DATA のサイズと異なる
MemoryOverflow	－	fileSize に 0 を入力する／ fileSize がバッファ領域サイズを超える

5.2.15 RestoreCard

APがICカードに対してファイル情報の書き戻しを指示するメッセージ.
APは本メッセージの生成時に，BackUpInfoメッセージで取得した保存ファイル情報backupinfoと，ファイル情報長backupinfolenと，署名signと，署名長signlenを指定する.
メッセージを受理したICカードは送信元の識別子と組である認証状態が所有者モードであれば，署名signの検証を行い，正しく検証されれば，
backupinfo内の乱数と自身が保持するrandomが等しいか照合を行い，等しければbackupinfoをICカードのメモリ領域へ書き戻す.

ICカードは，上記処理の正常終了時に，送信元にSuccessfulOperationメッセージを送信する.
ICカードは，上記処理の異常終了時に，送信元に以下のメッセージを送信する.
－LENと実際のDATAのサイズが異なる場合はIllegalParameterメッセージを送信する.
－送信元の識別子と組である認証状態が所有者モードでない場合は，AccessViolationメッセージを送信する.
－ファイル情報内の乱数とICカードがBackUpメッセージ実行時に保持している乱数が異なる場合とsignの検証に失敗した場合はIllegalParameterメッセージを送信する.
－ファイル情報内のfilenがICカードの格納可能最大ファイルを超える場合とカードの空き容量が無い場合はMemoryOverflowメッセージを送信する.

Parameters：

DATA詳細

Backupinfolen	ファイル情報長	2B
Signlen	署名長	2B
backupinfo	ファイル情報	(backupinfolen) B
sign	ICカードによる署名	(signlen) B

Output：

SuccessfulOperation

DATA詳細

MessageType	RestoreCardメッセージのMessageType	2B

Exceptional Output：

(エラーメッセージ)		(原因)
AccessViolation	－	ICカードがLOCKED状態である／ 送信元に対応する認証状態が所有者モードでない
IllegalParameters	－	LENがDATAのサイズと異なる／ ファイル情報内の乱数とICカードがBackUpCard時に保持している乱数の値が異なる／ signの検証に失敗
MemoryOverflow	－	ファイル情報内のファイル長であるfilenがICカードの格納可能最大ファイルを超える／ カードの空き容量が無い

5.3 IC カードからアプリケーションへの出力メッセージ

5.3.1 DelegatedID

IC カードが AP に対して ID を払い出すメッセージ.
本メッセージは RequestID メッセージに対する出力メッセージとして生成される.
IC カードは AP に払い出す識別子 AP_ID を DATA としてメッセージを生成する.

Parameters :

DATA 詳細		
AP_ID	AP に払い出す識別子	16B

5.3.2 Challenge

IC カードが AP に対してチャレンジデータを出力するメッセージ.
本メッセージは RequestChallenge メッセージに対する出力メッセージとして生成される.
IC カードはチャレンジである challengedata を DATA としてメッセージを生成する.

Parameters :

DATA 詳細

challengedata	チャレンジデータ	20B

5.3.3 AuthMode

IC カードが AP に対して遷移後の認証モードを出力するメッセージ.
本メッセージは Authenticate メッセージに対する出力メッセージとして生成される.
IC カードは遷移後の認証モードである mode を DATA としてメッセージを生成する.

Parameters :

DATA 詳細

mode	遷移後の認証モード 所有者モードに遷移：mode=0002h 非認証モードに遷移：mode=0000h	2B

5.3.4 SuccessfulFileOperation

IC カードが AP に対して，ファイルの作成／削除／移動のファイル操作結果を通知するメッセージ.

本メッセージは CreateFile メッセージ，DeleteFile メッセージ，MoveFile メッセージに対する出力メッセージとして生成される.

IC カードは処理を行ったメッセージの MessageType と，ファイルの識別子 fileID と，ファイル個数 fileCnt を DATA としてメッセージを生成する．fileCnt の意味はファイル操作により異なる.

- CreateFile メッセージに対しては，作成したファイルの個数を出力する.
- DeleteFile メッセージに対しては，削除したファイルの個数を出力する.
- moveFile メッセージに対しては，移動先のフォルダにおける現在のファイル個数を出力する.

Parameters：

DATA 詳細

MessageType	処理を行ったメッセージの MessageType	2B
fileID	作成／削除／移動先のファイルの識別子	2B
fileCnt	作成／削除／移動先のファイルの個数	4B

5.3.5 SuccessfulFolderOperation

IC カードが AP に対して，フォルダの作成／削除の操作結果を通知するメッセージ.

本メッセージは CreateFolder メッセージ，DeleteFolder メッセージに対する出力メッセージとして生成される.

IC カードは処理を行ったメッセージの MessageType と,作成／削除を行ったフォルダの識別子 folderID を DATA としてメッセージを生成する.

Parameters：

DATA 詳細

MessageType	処理を行ったメッセージの MessageType	2B
folderID	作成／削除を行ったフォルダの識別子	2B

5.3.6 SuccessfulOperation

IC カードが AP に対して，入力メッセージの処理の正常終了を通知するメッセージ.
本メッセージは ReformatCard メッセージ，RestoreCard メッセージ，CancelExchange メッセージに対する出力メッセージとして生成される.
IC カードは処理を行ったメッセージのメッセージタイプを DATA としてメッセージを生成する.

Parameters：

DATA 詳細

MessageType	処理を行ったメッセージの MessageType	2B

5.3.7 FileInfo

IC カードが AP に対して，ファイル情報を出力するメッセージ.

本メッセージは ReqeustFileInfo メッセージに対する出力メッセージとして生成される.

IC カードは，ファイルの内容である fileDATA とファイルの個数である fileCnt とファイルのアクセス権である fileACL とファイル生成者の識別子である issuerID と，読み出したファイル内容 fileDATA のサイズである readLen と実際のファイル長である filelen を DATA として，メッセージを生成する.

Parameters：

DATA 詳細

filelen	ファイルのデータ長 （実際のファイルのデータ長）	2B
fileCnt	ファイルの個数	4B
fileACL	ファイルのアクセス権	1B
issuerID	ファイル生成者の eTRON ID	16B
readLen	fileDATA のサイズ （読み出したファイルのデータ長）	2B
fileDATA	ファイルの内容	(readLen) B

5.3.8 FileList

IC カードが AP に対して，ファイルリストを出力するメッセージ.
本メッセージは ReqeustFileList メッセージに対する出力メッセージとして生成される.
IC カードは，フォルダリスト内のファイル個数である filenum と，filenum 個分のファイル情報を DATA とするメッセージを生成する.
ファイル情報は,ファイルの識別子 fileID とファイルの内容 fileDATA と,ファイルの個数 fileCnt と，ファイルのアクセス権 fileACL とファイルの生成者の識別子である issuerID と，読み出した fileDATA のサイズ readLen と，実際のファイル長である filelen である.

Parameters：

DATA 詳細

filenum	ファイルリストが管理するファイル個数	2B
fileinfo	ファイルのリスト	filenum*(27+readlen) B
fileID	ファイル識別子	2B
filelen	実際のファイルサイズ	2B
filecnt	ファイル個数	2B
fileACL	ファイル ACL	1B
issuerID	ファイル生成者の eTRON ID	16B
readlen	読み出したファイルデータの長さ	2B
fileDATA	読み出したファイルデータ	(readlen) B

5.3.9 FolderList

IC カードが AP に対して，フォルダリストを出力するメッセージ.
本メッセージは RequestFolderList メッセージに対する出力メッセージとして生成される.
IC カードはフォルダの個数である foldernum と，foldernum 個分のフォルダ情報を DATA とするメッセージを生成する.
フォルダ情報は,フォルダ識別子 folderID とフォルダ名 foldername とフォルダのアクセス権 folderACL である.

Parameters：

DATA 詳細

foldernum	フォルダの個数	2B
folderinfo	フォルダリスト	(foldernum*19)B
folderID	フォルダ識別子	2B
foldername	フォルダ名	16B
folderACL	フォルダ ACL	1B

5.3.10 CardInfo

IC カードが AP に対して，IC カード情報を出力するメッセージ.

本メッセージは RequestCardInfo メッセージに対する出力メッセージとして生成される.

IC カードは，カードへの書き込み可／不可を示す ICCState と，カードが実行可能な署名アルゴリズムである SignAlgorithm と，カードが実行可能な鍵のアルゴリズムである keyAlgorithm と，カードの公開鍵証明書である Cert と，生成可能最大フォルダ数 MaxFoldernum と，生成可能最大ファイル数 MaxFileNum と，生成可能最大ファイルサイズ MaxFileSize と，RequestCardInfo メッセージの送信元の AP の認証モードである authmode を DATA としてメッセージを生成する.

Parameters：

DATA 詳細

ICCState	ICC の状態	1B
SignAlgorithm	ICC が使用可能な署名のアルゴリズム	1B
KeyAlgorithm	ICC が使用可能な鍵のアルゴリズム	1B
Certlen	ICC の公開鍵証明書長	2B
Cert	ICC の公開鍵証明書	(Certlen) B
MaxFolderNum	生成可能最大フォルダ数	2B
MaxFileNum	生成可能最大ファイル数	2B
MaxFileSize	生成可能最大ファイルサイズ	2B
AuthMode	RequestCardInfo の Src の現在の認証モード	2B

5.3.11 BackUpInfo

IC カードが AP に対して，バックアップするファイル情報を出力するメッセージ.
本メッセージは BackUpCard メッセージに対する出力メッセージとして生成される.
IC カードは，ファイル情報と乱数の連結データである backupinfo と，backupinfo に対する IC カードの署名 sing と，署名長 signlen と，backupinfo のサイズ backupinfolen を DATA として，メッセージを生成する.

Parameters：

DATA 詳細

backupinfolen	ファイル情報長+乱数長	2B
signlen	署名長	2B
backupinfo	ファイル情報｜乱数	(backupinfolen) B
sign	IC カードによる backupinfo への署名	(signlen) B

5.3.12 UnsupportedMessage

IC カードが AP に対して，入力メッセージのメッセージタイプが規定値以外であることを通知するメッセージ.

errorCode はエラーの原因を示すメッセージ（情報）であり，内容は実装依存である.

Parameters :

DATA 詳細

errorCode	エラーの内容を示すメッセージ（情報）	2B
MessageType	処理を行ったメッセージの MessageType	2B

5.3.13 AccessViolation

IC カードが AP に対して，入力メッセージで指定されたフォルダやファイルへのアクセスを許可しないことを通知するメッセージ.

errorCode はエラーの原因を示すメッセージ（情報）であり，内容は実装依存である.

Parameters：

DATA 詳細

errorCode	エラーの内容を示すメッセージ（情報）	2B
MessageType	処理を行ったメッセージの MessageType	2B

5.3.14 ObjectNotFound

IC カードが AP に対して，入力メッセージで指定されたフォルダやファイルが存在しないことを通知するメッセージ.

errorCode はエラーの原因を示すメッセージ（情報）であり，内容は実装依存である.

Parameters :

DATA 詳細

errorCode	エラーの原因を示すメッセージ（情報）	2B
MessageType	処理を行ったメッセージの MessageType	2B

5.3.15 IllegalParameters

IC カードが AP に対して，入力メッセージのパラメータが不正であることを通知するメッセージ.
errorCode はエラーの原因を示すメッセージ（情報）であり，内容は実装依存である.

Parameters：

DATA 詳細

errorCode	エラーの原因を示すメッセージ（情報）	2B
MessageType	処理を行ったメッセージの MessageType	2B

5.3.16 MemoryOverflow

IC カードが AP に対して，入力メッセージの値が領域に関する上限／下限を超えることを通知するメッセージ.

errorCode はエラーの原因を示すメッセージ（情報）であり，内容は実装依存である.

Parameters：

DATA 詳細

errorCode	エラーの原因を示すメッセージ（情報）	2B
MessageType	処理を行ったメッセージの MessageType	2B

5.3.17 MaximumNumberExceeded

IC カードが AP に対して，入力メッセージのファイル個数などが上限／下限を超えることを通知するメッセージ.

errorCode はエラーの原因を示すメッセージ（情報）であり，内容は実装依存である.

Parameters：

DATA 詳細

errorCode	エラーの原因を示すメッセージ（情報）	2B
MessageType	処理を行ったメッセージの MessageType	2B

5.3.18 MessageSizeOverflow

IC カードが AP に対して，本来出力すべきメッセージの値が送受信可能なメッセージサイズを超えることを通知するメッセージ.

errorCode はエラーの原因を示すメッセージ（情報）であり，内容は実装依存である.

Parameters：

DATA 詳細

errorCode	エラーの原因を示すメッセージ（情報）	2B
MessageType	処理を行ったメッセージの MessageType	2B

5.3.19 ExchangeSuspended

IC カードが AP に対して，交換処理が途中で中断したことを通知するメッセージ.
errorCode はエラーの原因を示すメッセージ（情報）であり，内容は実装依存である.

Parameters：

DATA 詳細

errorCode	エラーの原因を示すメッセージ（情報）	2B
MessageType	処理を行ったメッセージの MessageType	2B

5.3.20 IncompatibleStatus

IC カードが AP に対して，入力メッセージの値で指定された交換処理が見つからないこと，または入力メッセージと現在の交換の状態の関係が整合しないことを通知するメッセージ.
errorCode はエラーの原因を示すメッセージ（情報）であり，内容は実装依存である.

Parameters：

DATA 詳細

errorCode	エラーの原因を示すメッセージ（情報）	2B
MessageType	処理を行ったメッセージの MessageType	2B

6 交換制御メッセージ

本章では，交換処理を行うためのメッセージ群およびデータフォーマットを規定する．6.1 節で交換を実現するプロトコルの詳細を説明する．6.2 節以降で交換制御のための各メッセージを規定する．

6.1 交換プロトコル詳細

本節では，本仕様書内の TENeT メッセージを搭載した TENeT IC カードが実現する安全かつ公平な交換機能について，採用した方式である「権利価値の楽観的な交換プロトコル」の詳細な動作を説明する．

6.1.1 登場人物

「権利価値の楽観的な交換プロトコル」の実行における登場人物は，権利価値の所有者と，権利価値が格納されている TENeT IC カード，および公平性を確保するための調停者サーバの役割をする TTP（Trusted Third Party）である．

交換プロトコルは2者間で実行されるため，権利価値の交換を提案する側と提案の受け手側が存在する．本章の説明では提案側を A，受け手側を B と記述する．提案側，受け手側共に TENeT IC カードと，所有者が操作する携帯端末上のアプリケーションプログラムがある．

本章では TENeT IC カードを ICC_X，アプリケーションプログラムを AP_X と記す．X は A，B のいずれかを示す．また ICC_X の識別子を ICC_XID，アプリケーションの識別子を AP_XID，TTP の識別子を ttpID とする．

登場人物の関係を図 1 に示す．

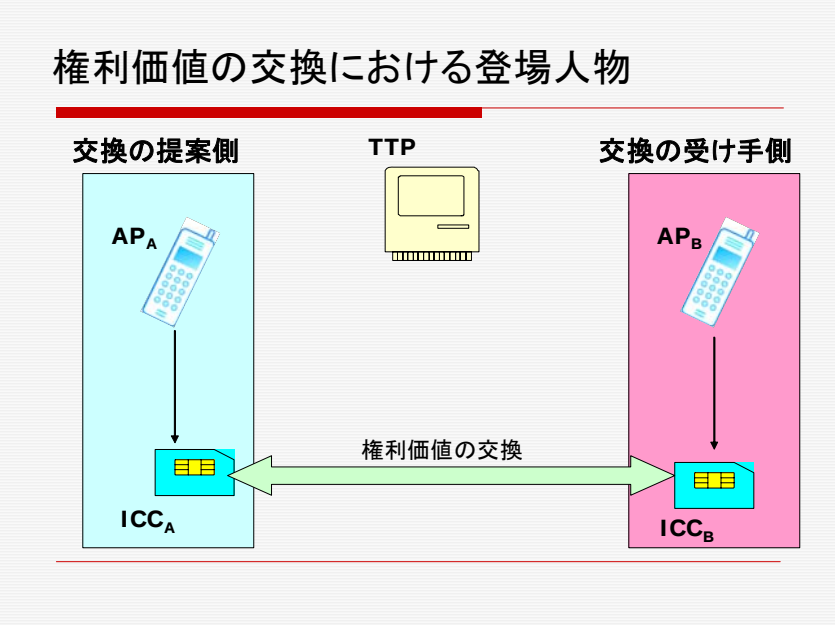

図 2　交換プロトコルの登場人物

6.1.2 プロトコル手順

本プロトコルは，主プロトコル，中止依頼プロトコル，完了依頼プロトコルで構成される．本節では各プロトコルの手順について説明する．

ICC_A と ICC_B は交換中の状態遷移を管理するセッション集合 S_A および S_B をそれぞれ保持し，TTP は完了許可済みの交換情報を保存する集合 $S_{resolve}$ と中止許可済みの交換情報を保存する集合 S_{abort} を保持する．

6.1.2.1 主プロトコル

交換プロトコルは，正常時には主プロトコルの実行により交換処理を完了する．以下に主プロトコルの手順を示す．

1. AP_A は，権利価値 v1 の条件と，交換対象である権利価値 v2 の条件を含む ConditionData を生成する．
2. AP_A は，ConditionData を含む交換の指示メッセージである **StartExchange** {AP_BID, ConditionData, ttpID} を生成して，ICC_A へ送付する．
3. ICC_A は，StartExchange 受理時に，乱数 n1 を生成して，n1 と ConditionData と ttpid を含む交換の提案メッセージ **Offer**{AP_AID, ConditionData, ttpid, n1}を生成して，AP_B へ送付する．
   ICCA は，Offer の送付後に，{ConditionData, ttpID, n1, tid}を Sa へ格納する．tid は StartExchange のヘッダに含まれるスレッド ID である（「e^2TP メッセージ仕様書」参照）．
4. AP_B は，Offer 受理時に，Offer に含まれる ConditionData を承諾するのであれば，ConditionData の条件に基づいて交換内容，すなわち v1 と v2 を確定し，**AgreeExchange** {AP_AID, ttpID, v1, v2, n1} を ICC_B へ送付する．
5. ICC_B は乱数 n2 と，提案内容識別情報である s1:＝h＜ttpid|v1|v2|n1＞と，
   セッション情報である s2:＝h＜n2＞を生成する．
   ICCB は，s1 と s2 の連結値(s1|s2)に対して自身の秘密鍵を用いて署名を行い，
   v2 を削除（退避）して，
   交換の承諾メッセージ **Agreement**：{ICC_BID, AP_BID, v1, v2, (s1|s2)P_{kB}, CertB} を生成して，AP_A へ送付する．
   AP_B は，Agreement の送付後に {v1, v2, n1, s1, s2, tid} を S_B へ格納する．Tid は
6. AP_A は，Agreement 受信時に，AP_B が確定した交換内容 v1 と v2 について，ConditionData の条件を満たしていることを確認すると，**ConfirmExchange**：{ICC_BID, AP_BID, v1, v2, (s1|s2)P_{kB}, CertB}を ICC_A へ送付する．
7. ICC_A は，ConfirmExchange 受信時に，(s1|s2)P_{KB} の署名検証が正しく行われれば，
   S_A に格納された ttpid と n1 と，受信した v1 と v2 を用いてハッシュ値 h<ttpid|v1|v2|n1>
   を生成し，s1 と生成したハッシュ値との照合を行う．
   ICC_A は，s1 と生成したハッシュ値が等しければ，v1 を削除し，自身の秘密鍵を用いて s2 に対して署名を行い，
   交換実行の指示である **Confirmation**：{AP_AID, AP_BID, (s2)P_{kA}, CertA} を ICC_B へ送付する．
   ICC_A は Confirmation の送付後に，{s1, s2} を S_A へ格納する．
8. ICC_B は Confirmation を受理する．
   ICC_B は，受理した(s2)P_{KA} の署名検証が正しく行われれば，
   s2 が S_B に格納されているセッション情報との照合を行う．
   ICCB は，s2 と等しい S_B 内のセッション情報があれば，
   交換対象である v1 を取得して，
   交換の完了である **Commitment**：{AP_AID, n2}を生成する．
   ICCB は S_B に格納した値を消去する．
   ICC_B は Commitment を ICC_A へ送付して，交換処理を完了する．
9. ICC_B は交換の完了通知である **ExchangeCommitted**：{ } を AP_B に送付する．
10. ICC_A は Commitment を受理する．
    ICC_A は受理した n2 のハッシュ値を生成して，S_A に格納されているセッション情報との照合を行う．
    ICC_A は，n2 のハッシュ値と等しい S_A 内のセッション情報があれば，
    交換対象である v2 を格納して，交換処理を完了する．
11. ICC_A は交換の完了通知である **ExchangeCommitted**：{ } を AP_A に送付する．
    ICCA は S_A に格納した値を消去する．

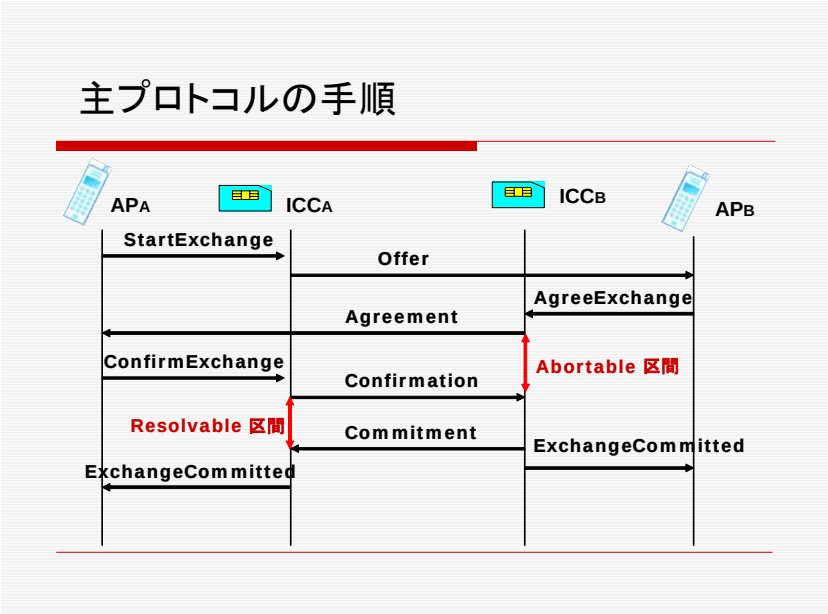

図 3　主プロトコル手順

図 2 に主プロトコルの手順を示す．図 2 の赤矢印部分の Resolvable/Abortable 区間は不公平な状態である．つまり，交換を行っている 2 者のうち一方のみが相手の権利価値を受け取っている状態，あるいは自分の権利価値を削除している状態である．この区間で処理が中断した場合には，それぞれの AP は相手との通信を再開せずに TTP との間で回復処理を行い，IC カードを上記の状態から，相手の状態に整合した公平な状態に回復させる．回復処理では，AP_X が ICC_X に中止/完了依頼プロトコルの実行を指示して，ICC_X と TTP 間で処理を行う．

具体的には，ICC_B は Abortable 区間（Agreement の送付から Confirmation の受理までの間）の任意の時点において，TTP との間で中止依頼プロトコルを実行して処理を中止（電子価値を復元）させることができる．同様に，ICC_A は Resolvable 区間（Confirmation の生成から Commitment の受理までの間）の任意の時点において，TTP との間で完了依頼プロトコルを実行することにより処理を終了させることができる．次節以降で，中止依頼プロトコルと完了依頼プロトコルの手順を説明する．

6.1.2.2 中止依頼プロトコル

交換プロトコルは異常終了時には中止依頼プロトコルの実行により，交換処理を終了する．中止依頼プロトコルの手順を図 3 に示す．

1. AP_B は，処理を中止したい交換の識別子 ExgThreadID を用いて，交換の中止を指示する **RecoverExchange**: {ExgThreadID} を生成し，ICC_B へ送付する．
2. ICC_B は RecoverExchange を受理し，
   SB に ExgThreadID と等しい tid があれば，
   SB 内の exgthreadiD に対応する s2 と，交換中止依頼を示すフラグである flag の連結値（flag|s2）に自身の秘密鍵を用いて署名を行い，
   交換中止依頼である **ArbitrationRequest**:{AP_BID, （flag|s2）P_{kB}, CertB}を生成して，
   SB 内の exgthreaidid に対応する ttpid を識別子とする TTP へ送付する．
3. TTP は ArbitrationRequest を受理し，署名の検証が正しく行われれば，
   - s2 が $S_{resolve}$ にない場合，
     交換中止依頼を示すフラグである flag と，受理した s2 の連結値（flag|s2）に自身の秘密鍵を用いて署名を行い，
     中止許可である **Arbitration**{AP_BID, （flag|s2)P_{kT},CertT} を ICC_B へ送付する．
     TTP は Arbitarion の送付後に s2 を S_{abort} へ格納する．
   - s2 が $S_{resolve}$ にある場合，

交換完了依頼を示すフラグである flag と，受理した s2 の連結値（flag|s2）に自身の秘密鍵を用いて署名を行い，
完了許可である **Arbitration**:{AP_BID, (flag|s2)P_{kT}, CertT} を ICC_B へ送付する．

4. ICC_B は Arbitration{(flag|s2)P_{kT},CertT}を受理して，署名検証後，s2 と等しい S_B 内のセッション情報があれば，
   - flag が中止許可を示していれば，
     V2 の復元後，交換の中止通知である **ExchangeAborted**：{} を AP_B に送付する．
   - flag が完了許可を示していれば，
     V1 の格納後，交換の完了通知である **ExchangeCommitted**：{} を AP_A に送付する．

   ICC_B は交換の中止／完了通知送信後，S_B に格納した値を消去する．

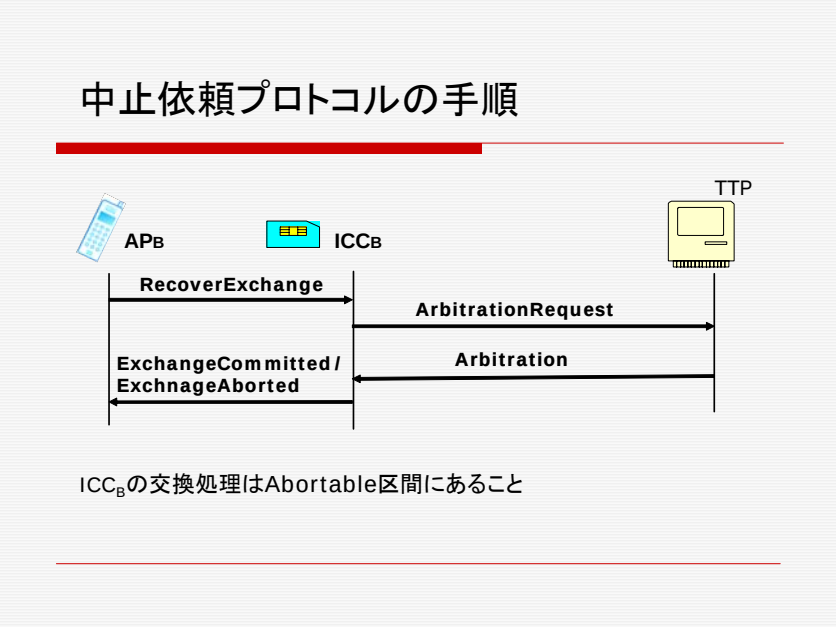

図 3 中止依頼プロトコル手順

6.1.2.3 完了依頼プロトコル

交換プロトコルは異常終了時には完了依頼プロトコルの実行により，交換処理を終了する．完了依頼プロトコルの手順を図 4 に示す．

1. AP_A は，処理を中止したい交換の識別子 ExgThreadID を用いて，交換の中止を指示する **RecoverExchange**:{ExgThreadID} を生成し，ICC_A へ送付する．
2. ICC_A は RecoverExchange を受理して，
   SA に ExgThreadID と等しい tid があれば，
   SB 内の exgthreadiD に対応する s2 と，交換中止依頼を示すフラグである flag の連結値（flag|s2）に自身の秘密鍵を用いて署名を行い，
   交換中止依頼である **ArbitrationRequest**:{AP_AID, (flag|s2) P_{kA}, CertA}を生成して，TTP へ送付する．
3. TTP は ArbitrationRequest を受理し，署名の検証が正しく行われれば，
   - s2 が S_{abort} にない場合，
     交換完了依頼を示すフラグである flag と，受理した s2 の連結値（flag|s2）に自身の秘密鍵を用いて署名を行い，
     完了許可である **Arbitration**{ AP_AID, (flag|s2)P_{kT},CertT} を ICC_A へ送付する．
     TTP は Arbitarion の送付後に s2 を $S_{resolve}$ へ格納する．
   - s2 が S_{abort} にある場合，
     交換中止依頼を示すフラグである flag と，受理した s2 の連結値（flag|s2）に自身の秘密鍵を用いて署名を行い，

中止許可である **Arbitration**:{AP_AID, (flag|s2)P_{kT}, CertT} を ICC_Aへ送付する.

4. ICC_Aは Arbitration{(flag|s2)P_{kT},CertT}を受理して，署名検証後，s2 と等しい S_A内のセッション情報があれば,
   - flag が中止許可を示していれば,
     V1 の復元後，交換の中止通知である **ExchangeAborted**：{} を AP_Aに送付する.
   - flag が完了許可を示していれば,
     V2 の格納後，交換の完了通知である **ExchangeCommitted**：{} を AP_Aに送付する.

   ICC_Aは交換の中止／完了通知送信後，S_Aに格納した値を消去する.

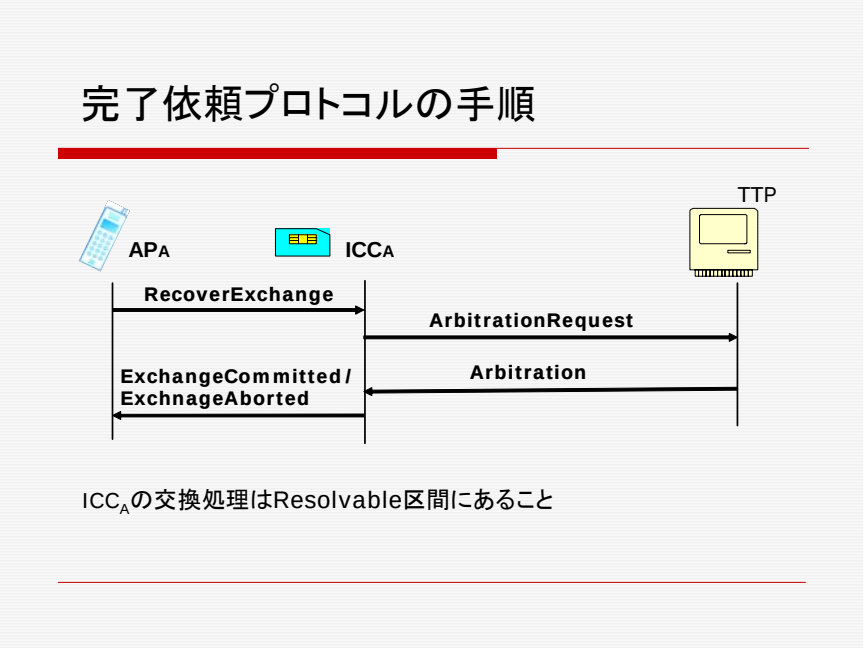

図 4 完了依頼プロトコル手順

6.2 ステートレコード／ステートテーブル

交換の提案側と受け手側の IC カードは交換処理で利用する情報をステートレコードとして管理する. IC カードは実行中の交換処理に対して表 11 に示すステートレコードで遷移状態と値を管理する. IC カードはステートレコードをメモリ上に連続して配置してステートテーブルとして管理する.

IC カードは交換処理が完了すると対応するステートレコードを開放する.

また，5.1.2 節の交換制御メッセージの状態遷移を表すステートレコードの state の値と交換処理の状態を表 12 に示す.

表 11 ステートレコード

#	データ	概要
1	state	交換処理の状態
2	exgtid	交換通常処理中のスレッド ID
3	ttpID	TTP の eTRON ID
4	s1	交換内容のハッシュ値
5	s2	乱数 n2 のハッシュ値
6	n1/n2	乱数
7	folderID	交換を行うフォルダのフォルダ ID
8	fileCnt1	交換元のファイルの個数
9	fileACL1	交換元のファイル ACL
10	issuerID1	交換元のファイルの発行者の eTRON ID
11	fileLen1	交換元のファイル長
12	fileData1	交換元のファイルデータ

13	fileCnt2	交換先のファイルの個数
14	fileACL2	交換先のファイル ACL
15	issuerID2	交換先のファイルの発行者の eTRON ID
16	fileLen2	交換先のファイル長
17	fileData2	交換先のファイルデータ

表 12 state の内容

#	state の値	交換処理の状態
1	None	初期状態（交換未開始）
2	Cancelable	Agreement 待ち状態
3	Abortable	Confirmation 待ち状態
4	Resolvable	Commitment 待ち状態
5	Wait_abort	中止許可待ち状態
6	Wait_commit	完了許可待ち状態

6.3 アプリケーション／IC カードから IC カードへの入力メッセージ

6.3.1 主プロトコルメッセージ

6.3.1.1 StartExchange

AP_A が ICC_A に対して交換の開始を指示するメッセージ.

AP_A は本メッセージの入力時に，交換相手の AP_A の識別子 AP_AID と，TTP の識別子 ttpID と，交換条件 ConditionData を指定する．(6.1.2 節参照)

ICC_A は，本メッセージの送信元の識別子に対応する認証状態が所有者モードである時，かつ e^2TP メッセージに含まれるスレッド ID である tid と同一のスレッド ID を持つステートレコードがない時に，
乱数 n1 を生成して，識別子が AP_BID である AP_B に対して本メッセージの送信元の識別子 AP_AID と調停サーバの識別子 ttpID と交換条件 ConditionDATA を含む Offer メッセージを送信する.

ICC_A は，steta が Cancelrable であり，{ConditionData, ttpID, n1, tid}を持つ新しいステートレコードを生成する.

ICC_A は,Offer メッセージの出力後,state が Calcelable であり,n1 と tid と tppid および ConditionData を持つステートレコードを生成する.

また ICC_A は，上記処理の異常終了時に，AP_A に以下のメッセージを送信する.

- e^2TP メッセージに含まれる LEN と DATA のサイズが異なる場合は IllegalParameters メッセージを送信する.
- 送信元の識別子に対応する認証状態が所有者モードない場合は AccessViolation メッセージを出力する.
- ステートレコードを生成する空き領域がない場合は MemoryOverflow メッセージを出力する.
- tid を同じスレッド ID を持つステートレコードが既に存在する場合は IncompatibleStatus メッセージを出力する.

Parameters :

DATA 詳細

AP_AID	AP_B の識別子	16B
ttpID	TTP の eTRON ID	16B
ConditionDataSize	コンディションデータサイズ	2B
ConditionData	コンディションデータ	(ConditionDATASize) B

Output :

Offer

DATA 詳細

AP_AID	AP_A の識別子	16B
ttpID	TTP の eTRON ID	16B
ConditionDataSize	コンディションデータサイズ	2B
ConditionData	コンディションデータ	(ConditionDATASize) B
n1	乱数	20B

Exceptional Output :

(エラーメッセージ)	(原因)
AccessViolation	－ IC カードが LOCKED 状態である／ 送信元に対応する認証状態が所有者モードでない
IllegalParameters	－ LEN が DATA のサイズと異なる
MemoryOverflow	－ カードの空き容量がない

IncompatibleStatus　　－　同一 ThreadID のステートレコードが既に存在する／

6.3.1.2 Offer

ICC_AがAP_Bに対して交換の提案を行うメッセージ.

ICC_Aは，StartExchange の送信元の識別子 AP_AID と，TTP の識別子 ttpID と，提案内容 ConditionDATA と乱数 n1 を DATA としてメッセージを生成する.

AP_Bは，Offer メッセージを受理後，ConditionDATA である提案内容に承諾すると，ICC_Bに対して Offer の DATA の値をそのまま入力とする AgreeExchange メッセージを出力する.

Parameters：

DATA 詳細

AP_AID	AP_Aの識別子	16B
ttpID	TTP の eTRON ID	16B
ConditionDataSize	コンディションデータサイズ	2B
ConditionData	コンディションデータ	(ConditionDATASize) B
n1	乱数	20B

6.3.1.3 AgreeExchange

AP_B が ICC_A に対して交換の開始を指示するメッセージ.

AP_B は本メッセージの入力時に，StartExchange の送信元の識別子 AP_AID と，TTP の識別子 ttpid と，AP_B が確定した交換内容（交換の提案元のファイル内容 v1 と個数 num1 とサイズ size1 とアクセス権 acl1 と生成者識別子 issuerID1 と v1 の格納元フォルダ識別子 folderid1， 交換の受け手側のファイル内容 v2 と個数 num2 とサイズ size2 とアクセス権 acl2 と生成者識別子 issuerID2 と v2 の格納元のフォルダ識別子 folderid2）と，乱数 n1 を指定する.

ICC_B は，送信元の識別子に対応する認証状態が所有者モードである時，かつ e^2TP メッセージに含まれるスレッド ID である tid と同一のスレッド ID を持つステートレコードがない時，かつ v2 の transfer 権限が許可されている時に，乱数 n2 を生成して，提案内容識別情報 s1:=h<v1|v2|n1>と，セッション情報 s2:=h<n2>を生成する.

ICC_B は v2 の情報をフォルダから削除（退避）して，s1 と s2 を連結した値 msg:=（s1|s2）と，msg に対する署名 sign:=(s1|s2)P_{KB} と，公開鍵証明書 CertB と，v1 と v2 の情報と，交換の受け手側の識別子 ICC_BID と AP_BID を含む Agreement メッセージを出力する.

ICC_B は，Agreement の出力後，state が Abortable であり，{n2，s1，s2，tid，tppID と v1 と v2 の情報} を持つステートレコードを生成する.

また ICC_B は，上記処理の異常終了時に，AP_B に以下のメッセージを送信する.

- LEN と DATA のサイズが異なる場合と，num1 と num2 に共に 0 を入力した場合は IllegalParameters メッセージを送信する.
- 送信元の識別子と組である認証状態が所有者モードでない場合は AccessViolation メッセージを送信する.
- ステートレコードを生成する空き領域がない場合は MemoryOverflow メッセージを送信する.
- 同一 ThreadID を持つステートレコードが既に存在する場合は IncompatibleStatus メッセージを送信する.
- 指定されたフォルダやファイルが存在しない場合は ObjectNotFound メッセージを送信する.
- v2 の個数が num2 より少ない場合は MaximumNumberExceeded メッセージを送信する.

Parameters：

DATA 詳細

AP_AID	AP_A の識別子	16B
ttpID	TTP の eTRON ID	16B
folderID1	v1 の格納先のフォルダ ID	2B
folderID2	v2 の格納元のフォルダ ID	2B
num1	ファイル v1 の個数	4B
acl1	ファイル v1 の ACL	1B
issuerid1	ファイル v1 の発行者の eTRON ID	16B
size1	ファイル v1 のファイルサイズ	2B
v1	ファイル v1 の本体	(size1) B
num2	ファイル v2 の個数	4B
acl2	ファイル v2 の ACL	1B
issuerid2	ファイル v2 の発行者の eTRON ID	16B
size2	ファイル v2 のファイルサイズ	2B
v2	ファイル v2 の本体	(size2) B
n1	乱数	20B

Output：

Agreement

DATA 詳細

ICC_BID	Recipient 側 ICC の eTRON ID	16B
AP_BID	Recipient 側 AP の識別子	16B
msglen	msg 長	2B
signlen	sign 長	2B
Certlen	Recipient 側の公開鍵証明書のサイズ	2B
msg	署名対象となった（s1｜s2）	(msglen) B
sign	署名	(signlen) B
CertB	Recipient 側の公開鍵証明書	(Certlen) B
num1	ファイル v1 の個数	4B
acl1	ファイル v1 の ACL	1B
issuerid1	ファイル v1 の発行者 ID	16B
size1	ファイル v1 のファイルサイズ	2B
v1	ファイル v1 の本体	(size1) B
num2	ファイル v2 の個数	4B
acl2	ファイル v2 の ACL	1B
issuerid2	ファイル v2 の発行者 ID	16B
size2	ファイル v2 のファイルサイズ	2B
v2	ファイル v2 の本体	(size2) B

Exceptional Output：

（エラーメッセージ）	（原因）
AccessViolation	－ IC カードが LOCKED 状態である／ 送信元に対応する認証状態が所有者モードでない／ v2 で示されるファイルの transfer 権が認められていない
ObjectNotFound	－ folderid で示されるフォルダが存在しない／ {acl2,issuerid2,size2,v2} で示されるファイルが存在しない
IllegalParameters	－ LEN が DATA のサイズと異なる／ num1 と num2 に共に 0 を入力する
MemoryOverflow	－ v1 のファイルサイズである size1 が格納可能最大ファイル長を超える／ カードの空き容量がない
MaximumNumberExceeded	－ 指定された v2 の Cnt が num2 より少ない
IncompatibleStatus	－ 同一の ThreadID が既に存在する

6.3.1.4 Agreement

ICC_BがAP_Aに対して交換の提案内容への合意を示すメッセージ.

ICC_Bは，AgreeExchange の送信元の識別子AP_BID と，本メッセージの送信元の識別子ICC_BID と，交換の識別子 s1 と s2 を連結した値 msg と，ICC_Bが msg に付与した署名 sign と，ICC_Bの公開鍵証明書 CertB と，交換するファイル v1 と v2 の情報を DATA として，メッセージを生成する.

AP_Aは確定した v1 と v2 の内容が ConditionData の条件を満たしていることを確認すると，ICC_Aに対して Agrrement の DATA をそのまま入力とする ConfirmExchange メッセージを送信する.

Parameters：

DATA 詳細

ICC_BID	ICC_Bの eTRON ID	16B
AP_BID	AP_Bの識別子	16B
msglen	msg 長	2B
signlen	sign 長	2B
Certlen	Recipient 側の公開鍵証明書のサイズ	2B
msg	署名対象となった（s1｜s2）	(msglen) B
sign	署名	(signlen) B
CertB	Recipient 側の公開鍵証明書	(Certlen) B
num1	ファイル v1 の個数	4B
acl1	ファイル v1 の ACL	1B
issuerid1	ファイル v1 の発行者 ID	16B
size1	ファイル v1 のファイルサイズ	2B
v1	ファイル v1 の本体	(size1) B
num2	ファイル v2 の個数	4B
acl2	ファイル v2 の ACL	1B
issuerid2	ファイル v2 の発行者 ID	16B
size2	ファイル v2 のファイルサイズ	2B
v2	ファイル v2 の本体	(size2) B

6.3.1.5 ConfirmExchange

AP_A が ICC_A に対して確定した交換の継続を指示するメッセージ．AP_A は本メッセージの入力時に，AgreeExchange メッセージの送信元の識別子 AP_BID と，Agreement メッセージの送信元の識別子 ICC_BID と，s1 と s2 の連結データ msg と，msg に付与された署名 sign と，ファイル v1 と v2 の情報を指定する．

ICC_Aは，送信元の識別子に対応する認証状態が所有者モードである時，かつ e^2TP メッセージに含まれるスレッド ID である tid と同一のスレッド ID を持つステートレコードがない時，かつファイル v1 の transfer 権限が許可されている場合のみメッセージを受理する．

ICC_Aは msg に付与された署名 sign の検証を行う．署名が正しく検証されれば，msg から s1 を取り出し，ステートレコードに格納された ttpid と n1 と，受信した v1 と v2 を用いてハッシュ値 h<ttpid|v1|v2|n1> を生成し，s1 と生成したハッシュ値との照合を行う．

照合が正しく行われれば，v1 をフォルダから削除（退避）して，ICC_Bに対して s1 と s2 に付与する署名 sign と ICC_Aの公開鍵証明書 CertA と本メッセージの送信元の識別子 AP_AID と AgreeExchange の送信元の識別子 AP_BID を含む Confirmation を送信する．

Confirmation の出力後，ICC_A は tid と等しいスレッド ID を持つステートレコードの state 値を Cancelable から Resolvable へ更新する．
ICC_Aは，tid を含むステートレコードの state を Cancelable から Resolvable へ更新し，ファイル情報 v1 と v2 と交換の識別子 s1 と s2 を格納する．

また ICC_Aは，上記処理の異常終了時に，AP_Aに以下のメッセージを送信する．
－ LEN と DATA のサイズが異なる場合と，
num1 と num2 に共に 0 を入力した場合と，
送信元の識別子と組である認証状態が所有者モードではない場合と，
指定されたフォルダやファイルが存在しない場合と，
署名付与や署名検証に失敗した場合は，
ExchangeSuspended メッセージを送信する．

Parameters：

DATA 詳細

ICC_BID	ICC_Bの eTRON ID 16B	
AP_BID	AP_Bの eTRON ID 16B	
msglen	msg 長	2B
siglen	署名長	2B
certlen	Recipient 側の公開鍵証明書のサイズ	2B
msg	署名対象となった（s1｜s2）	(msglen) B
sign	署名	(signlen) B
CertB	Recipient 側の公開鍵証明書	(Certlen) B
folderID1	v1 の格納元のフォルダ ID	2B
folderID2	v2 の格納先のフォルダ ID	2B
num1	ファイル v1 の個数	4B
acl1	ファイル v1 の ACL	1B
issuerid1	ファイル v1 の発行者 ID	16B
size1	ファイル v1 のファイルサイズ	2B
v1	ファイル v1 の本体	(size1) B
num2	ファイル v2 の個数	4B
acl2	ファイル v2 の ACL	1B
issuerid2	ファイル v2 の発行者 ID	16B
size2	ファイル v2 のファイルサイズ	2B
v2	ファイル v2 の本体	(size2) B

Output :

Confirmation

DATA 詳細

OriginAPID	Originator 側 AP の eTRON ID	16B
RecipientAPID	Recipient 側 AP の eTRON ID	16B
msglen	msg 長	2B
siglen	sign 長	2B
certlen	Originator 側の公開鍵証明書のサイズ	2B
msg	署名対象となった s2	(msglen) B
sign	署名	(signlen) B
CertA	Originator 側の公開鍵証明書	(certlen) B

Exceptional Output :

(エラーメッセージ)	(原因)
ExchangeSuspended	ー IC カードが LOCKED 状態である／ LEN が DATA のサイズと異なる／ 送信元に対応する認証状態が所有者モードでない／ ファイル v1 の Transfer 権が認められていない／ folderid1 で示されるフォルダが存在しない／ {acl1,issuerid1,size1,v1} であるファイルが存在しない／ num1 と num2 に共に 0 を入力する／ Cert のフォーマットが異なる／ Cert の検証に失敗／ 署名の検証に失敗／

6.3.1.6 Confirmation

ICC_AがICC_Bに対して確定した交換内容への合意を示すメッセージ.

ICC_Aは，ConfirmExchange の送信元の識別子 AP_AID と AgreeExchange の送信元の識別子 AP_BID と，交換の識別子 s2 を含む msg と，msg に対する署名 sign を DATA として，本メッセージを生成する.

ICC_Bは,e^2TP メッセージのスレッド ID である tid と同一のスレッド ID を持つステートレコードの state 値が Abortable である場合，msg に付与された署名 sign の検証を行う．ICC_Bは，署名が正しく検証されれば，v1 を取得して，ICC_Aに対して Commitment を送信する．また ICC_Bから AP_Bに対して交換の完了を通知する ExchangedCommitted を送信する.

ICC_Bは，tid を含むステートレコードを削除する（state 値を None に更新する).

Commitment/ExchangeCommitted の送信後，ICC_Bは tid と同一のスレッド ID を持つステートレコードを解放する.

また ICC_Bは，上記処理の異常終了時に，AP_Bに以下のメッセージを送信する.

－ LEN と DATA のサイズが異なる場合と，
Parameter の値が対応するデータサイズと異なる場合と，
署名の検証に失敗した場合と，
ICC_Bに v1 が既に存在し，かつ num1 の加算結果が上限を超える場合と，
ICC_Bに v1 が存在せず，かつファイルに空き容量が無い場合は，
ExchangeSuspended メッセージを送信する.

Parameters：

DATA 詳細

AP_AID	AP_Aの識別子	16B
AP_BID	AP_Bの識別子	16B
msglen	msg 長	2B
siglen	sign 長	2B
certlen	Originator 側の公開鍵証明書のサイズ	2B
msg	署名対象となった s2	(msglen) B
sign	署名	(signlen) B
CertA	Originator 側の公開鍵証明書	(certlen) B

Output：

ExchangeCommitted　－ ICC_Aへ送信

DATA 詳細

なし

Commitment　－ AP_Bへ送信

DATA 詳細

AP_AID	AP_Aの識別子	16B
n2	乱数	20B

Exceptional Output：

(エラーメッセージ)	(原因)
ExchangSuspended	－ IC カードが LOCKED 状態である／ 送信元に対応する認証状態が所有者モードでない／ LEN が DATA のサイズと異なる／ msglen,siglen,certlen の値がデータと異なる／ Cert のフォーマットが異なる／

Cert の検証に失敗／
署名の検証に失敗／
ファイル v1 の加算結果が FFFFFFFFFh を超える／
カードの空き容量が存在しない／
スレッド ID が等しいステートレコードが存在しない／
スレッド ID が等しいステートレコード内の s2 と受信した s2 が不一致

6.3.1.7 Commitment

ICC_BがICC_Aに対して v1 の取得を通知するメッセージ．ICC_Bは，StartExchange の送信元の識別子AP_AID と乱数 n2 を DATA として本メッセージを生成する．

ICC_Aはe^2TP メッセージのスレッド ID である tid と同一の ExgThreadID を持つステートレコードの state 値が Resolvable である時，n2 のハッシュ値 h＜n2＞とステートレコード内の s2 が等しいか照合を行う．

等しい場合は，v2 を取得して，AP_Aに対して交換の完了を通知する ExchangeCommitted を送信する．ICC_Aは，tid を含むステートレコードを削除する（state 値を None に更新する）．

またICC_Bは，上記処理の異常終了時に，AP_Bに以下のメッセージを送信する．

－ LEN と DATA のサイズが異なる場合と，
ICC_Bにファイル v2 が既に存在し，かつ num2 の加算結果が上限を超える場合と，
ICC_Bにファイル v2 が存在せず，かつファイルに空き容量が無い場合は，
ExchangeSuspended メッセージを送信する．

Parameters：

DATA 詳細		
AP_AID	APA の識別子	16B
n2	乱数 n2	20B

Output：

ExchangedCommited

DATA 詳細

なし

Exceptional Output：

ExchangSuspended	－ IC カードが LOCKED 状態である／ LEN が DATA のサイズと異なる／ ファイル v2 の個数の加算結果が FFFFFFFFh を超える／ カードの空き容量が存在しない

6.3.2 中止依頼／完了依頼プロトコルメッセージ

6.3.2.1 RecoverExchange

AP_X が ICC_X に対して中止依頼／完了依頼を指示するメッセージ.

ICC_X は送信元の識別子に対応する認証状態が所有者モードであれば，ExgThreadID を含むステートレコードの state 値に従って処理を行う.

ICC_X は，state が Cancelable であれば，送信元の AP に ExchangeAborted メッセージを送信する. ICCXha，ExchangeAborted メッセージの送信後，ExgThreadID を含むステートレコードを解放する.

ICCX は，state が Abortable か Wait_Abort であれば，中止依頼プロトコルを実行する.ICCX は，state が Resolvable か Wait_Commit であれば，完了依頼プロトコルを実行する. (6.1.2 節 参照)

ICC_X は，中止依頼と完了依頼を識別するフラグ flag とセッション識別子 s2 を連結した（flag|s2）である msg と，msg に対する署名 sign と，本メッセージの送信元の識別子と，ICC_X の公開鍵証明書 CertX を含む ArbitrationRequest メッセージを送信する.

また ICC_X は，上記処理の異常終了時に，AP_X に以下のメッセージを送信する.

－ LEN と DATA のサイズが異なる場合と，
SrcID が所有者として認証されていない場合と，
受信した ExgThreadID と同じスレッド ID を持つステートレコードが存在しない場合と，
state の値が規定値以外の値である場合は，
ExchangeSuspended メッセージを送信する.

Parameters :

DATA 詳細

ExgThreadID	復旧対象交換内容の ExgThreadID	16B

Output :

ArbitrationRequest

DATA 詳細

RecoverAPID	RecoverExchange の送信元の識別子	16B
msglen	msg 長	2B
signlen	sign 長	2B
certlen	X の公開鍵証明書のサイズ	2B
msg	署名対象となった（flag(*)｜s2）	(msglen) B
sign	署名	(signlen) B
CertX	X の公開鍵証明書	(certlen) B

(*)flag について
flag = 0 ： 中止依頼
flag = 1 ： 完了依頼

ExchangeAborted

DATA 詳細

なし

Exceptional Output :

（エラーメッセージ）	（原因）
ExchangSuspended	－ IC カードが LOCKED 状態である／LEN が DATA のサイズと異なる／ － 送信元に対応する認証状態が所有者モードでない／ － ExgThreadID と同一のスレッド ID を持つステートレコードが存在しない

－ state の値が規定値以外の値である／

6.3.2.2 ArbitrationRequest

ICC_Xが，TTP に対して完了依頼または中止依頼を行うメッセージ.

ICC_Xは，RecoverExchange の送信元の識別子 AP_XID と，交換の識別子 s2 と，メッセージの送信元の識別子と，中止依頼／回復依頼を分類するフラグ flag とセッション情報 s2 の連結値 msg と，msg に対する署名 sign と，ICC_Xの公開鍵証明書 CertX を指定する.

TTP は，本メッセージの受信後，ArbitrationRequest の送信元の識別子 ICC_XID に対して Arbitration メッセージを送信する.

Parameters：

DATA 詳細

RecoverAPID	RecoverExchange の SrcID	16B
msglen	msg 長	2B
signlen	sign 長	2B
certlen	X の公開鍵証明書のサイズ	2B
msg	署名対象となった（flag(*)｜s2)	(msglen) B
sign	署名	(signlen) B
CertX	X の公開鍵証明書	(certlen) B

(*)flag について

flag = 0 ： 中止依頼

flag = 1 ： 完了依頼

6.3.2.3 Arbitration

TTP が ICC_X に対して中止許可または完了許可を与えるメッセージ.

TTP は，RecoverExchange の送信元の識別子 AP_XID と，セッション識別子 s2 と中止依頼／回復依頼を分類するフラグ flag の連結値 msg と，msg に対する署名 sign を DATA として，メッセージを生成する.

ICC_Xは，s2 を含むステートレコードの state 値が Wait_Commit，Wait_Abort である時に，署名 sign の検証を行う.

署名 sign が正しく検証された場合に,

flag が中止許可であれば,

－ICC_Aであれば退避した v1 を復元して AP_Aに対して ExchangeAborted を送信する.
ExchangeAborted メッセージの送信後，s2 を含むステートレコードを解放する.

－ICC_Bであれば退避した v2 を復元して AP_Bに対して ExchangeAborted を送信する
ExchangeAborted メッセージの送信後，s2 を含むステートレコードを解放する.

flag が完了許可であれば,

－ICC_Aであれば v2 を取得して AP_Aに対して ExchangeCommitted を送信する.
ExchangeCommitted メッセージの送信後，s2 を含むステートレコードを解放する.

－ICC_Bであれば v1 を取得して AP_Bに対して ExchangeCommitted を送信する
ExchangeCommitted メッセージの送信後，s2 を含むステートレコードを解放する.

ExchangeCommitted/ExchangeAborted の送信後,ICC_Aは e2TP メッセージの ThreadID と同一の ThreadID を持つステートレコードを解放する.

また ICC_Bは，上記処理の異常終了時に，AP_Bに以下のメッセージを送信する.

－ LEN と DATA のサイズが異なる場合は，ExchangeSuspended メッセージを送信する.

－ s2 を含むステートレコードが存在しない場合と,
S2 を含むステートレコードの state 値が Wait_Commit か Wait_Abort でない場合は,
IncompatibleStatus メッセージを送信する.

Parameters：

DATA 詳細

RecoverAPID	RecoverExchange の送信元の識別子	16B
msglen	msg 長	2B
signlen	sign 長	2B
certlen	TTP の公開鍵証明書のサイズ	2B
msg	署名対象となった（flag(*)｜s2）	(msglen) B
sign	署名	(signlen) B
CertT	TTP の公開鍵証明書	(certlen) B

(*)flag について

flag = 0 ： 中止許可
flag = 1 ： 完了許可

Output：

ExchangeCommited

DATA 詳細

なし

ExchangeAborted

DATA 詳細

なし

Exceptional Output :

(エラーメッセージ)		(原因)
ExchangSuspended	－	IC カードが LOCKED 状態である／ 送信元に対応する認証状態が所有者モードでない／ LEN が DATA のサイズと異なる
IncompatibleStatus	－	交換処理が存在しない／交換途中状態が不正

6.3.2.4 CancelExchange

AP_A が ICC_A に対して，state が Cancelable 区間である交換処理の中止を指示するメッセージ.
AP_A は本メッセージの入力時に中止する交換処理のスレッド ID である ChkThreadID を指定する.
ICC_A は処理が正常に終了すると，ExchangeAborted を送信する．ExchangeAborted の送信後，ICC_A は ChkThreadID を含むステートレコードを解放する.
また ICC_B は，LEN と DATA のサイズが異なる場合は，AccessViolation メッセージを送信する.
ChkThreadID と同一のスレッド ID を含むステートレコードが存在しない場合と，
ChkThreadID と同一のスレッド ID を含むステートレコードの state が Cancelable でない場合は，
IncompatibleStatus メッセージを送信する.

Parameters：

DATA 詳細

ChkThreadID	中止する交換処理の ThreadID	20B

Output：

ExchangeAborted

DATA 詳細

MessageType	処理を行ったメッセージの MessageType	2B

Exceptional Output：

(エラーメッセージ)		(原因)
AccessViolation	－	IC カードが LOCKED 状態である／ 送信元に対応する認証状態が所有者モードでない
IncompatibleStatus	－	ChkThreadID を含むステートレコードが存在しない／ state が Cancelable ではない
IllegalParameters	－	LEN が DATA のサイズと異なる

6.3.3 交換状態管理メッセージ

6.3.3.1 RequestExgStatusInfo

AP_X が ICC_X に対して指定したスレッド ID を識別子として持つ交換処理の情報を取得するメッセージ. AP_X は本メッセージの入力時に，検索するスレッド ID である ChkThreadID を指定する.

ICC_X は送信元の識別子に対応する認証状態が所有者モードであれば，交換するファイル v1 と v2 および交換状態 state とスレッド ID である ExgThreadID を含む ExgStatusInfo を送信する.ExchangeStatusInfo に含まれるデータは，state が Cancelable である場合とそれ以外の場合で異なる.

また ICC_X は，上記処理の異常終了時に，AP_X に以下のメッセージを送信する.

- LEN と DATA のサイズが異なる場合は，IllegalParameters メッセージを送信する.
- 送信元の識別子と組である認証状態が所有者モードでない場合は，AccessViolation メッセージを送信する.
- ChkThreadID で示されるステートレコードがない場合は，ObjectNotFound メッセージを送信する.

Parameters :

DATA 詳細

ChkThreadID	検索する ThreadID	20B

Output :

ExgStatusInfo

DATA 詳細

(state = Cancelable の場合)

status	検索した交換内容の state	1B
ExgThreadID	検索した交換内容のスレッド ID	20B
ttpID	検索した交換内容の ttpid	16B
folderID1	検索した交換内容の folderID1	2B
folderID2	検索した交換内容の folderID2	2B
ConditionDataSize	コンディションデータのサイズ	2B
ConditionData	コンディションデータ	(CondiotonDataSize) B

(state = Cancelable 以外の場合)

status	検索した交換内容の state	1B
ExgThreadID	検索した交換内容のスレッド ID	20B
ttpID	検索した交換内容の ttpid	16B
folderID1	検索した交換内容の folderID1	2B
folderID2	検索した交換内容の folderID2	2B
num1	検索した交換内容の v1 の num	4B
acl1	検索した交換内容の v1 の acl	1B
issuerid1	検索した交換内容の v1 の issuerid	16B
size1	検索した交換内容の v1 の size	2B
v1	検索した交換内容の v1 の内容	(size1) B
num2	検索した交換内容の v2 の num	4B
acl2	検索した交換内容の v2 の acl	1B
issuerid2	検索した交換内容の v2 の issuerid	16B
size2	検索した交換内容の v2 の size	2B
v2	検索した交換内容の v2 の内容	(size2) B

Exceptional Output：

（エラーメッセージ）		（原因）
AccessViolation	－	IC カードが LOCKED 状態である／ 送信元に対応する認証状態が所有者モードでない
ObjectNotFound	－	ChkThreadID で示されるステートレコードが存在しない
IllegalParameters	－	LEN が DATA のサイズと異なる

6.3.3.2 RequestExgStatusList

AP_X が ICC_X に対してスレッド ID のリストの送信を要求するメッセージ.
AP_X は本メッセージの生成時に指定する値は空である.

ICC_X は送信元の識別子に対応する認証状態が所有者モードであれば，交換中のスレッド ID である ExhThreadID と交換状態である state を組としたリスト ExgStatusList を送信する.
また ICC_X は，上記処理の異常終了時に，AP_X に以下のメッセージを送信する.
- LEN と DATA のサイズが異なる場合は，IllegalParameters メッセージを送信する.
- 送信元の識別子に対応する認証状態が所有者モードでない場合は，AccessViolation メッセージを送信する.
- ChkThreadID を含むステートレコードがない場合は，ObjectNotFound メッセージを送信する.

Parameters :

DATA 詳細
なし

Output :

ExgStatusList
DATA 詳細

ThreadIDList	スレッド ID リスト	
ThreadIDNum	交換内容の個数	2B
ThreadIDInfo	交換内容のリスト	
state	状態管理パラメータ	1B
ExgThreadID	交換正常処理中のスレッド ID	20B

Exceptional Output :

(エラーメッセージ)	(原因)
AccessViolation	－ IC カードが LOCKED 状態である／送信元に対応する認証状態が所有者モードでない
IllegalParameters	－ LEN が DATA のサイズと異なる

6.4 IC カードからアプリケーションへの出力メッセージ

6.4.1 ExchangeCommitted

ICC_X が AP_X に対して，交換処理が完了したことを通知するメッセージ．ICC_X は DATA と空としてメッセージを生成する．

Parameters：

DATA 詳細

なし

6.4.2 ExchangAborted

ICC_XがAP_Xに対して，交換処理が中止したことを通知するメッセージ．ICC_XはDATAを空としてメッセージを生成する．

Parameters：

DATA 詳細

なし

6.4.3 ExgStatusInfo

ICC_X が AP_X に対して，交換処理の状態を通知するメッセージ.
本メッセージは RequestExgStatusInfo メッセージに対する出力メッセージとして生成される.
ICC_X は検索した ThreadID を含む交換処理の情報を DATA としてメッセージを生成する.

Parameters：

DATA 詳細

(state = Cancelable の場合)

status	検索した交換内容の state	1B
ExgThreadID	検索した交換内容の ExgThreadID	20B
ttpID	検索した交換内容の ttpid	16B
folderID1	検索した交換内容の folderID 1	2B
folderID2	検索した交換内容の folderID 2	2B
ConditionDataSize	コンディションデータのサイズ	2B
ConditionData	コンディションデータ	(CondiotonDataSize) B

(state = Cancelable 以外の場合)

status	検索した交換内容の state	1B
ExgThreadID	検索した交換内容の ExgThreadID	20B
ttpID	検索した交換内容の ttpid	16B
folderID1	検索した交換内容の folderID 1	2B
folderID2	検索した交換内容の folderID 2	2B
num1	検索した交換内容の v1 の num	4B
acl1	検索した交換内容の v1 の acl	1B
issuerid1	検索した交換内容の v1 の issuerid	16B
size1	検索した交換内容の v1 の size	2B
v1	検索した交換内容の v1 の内容	(size1) B
num2	検索した交換内容の v2 の num	4B
acl2	検索した交換内容の v2 の acl	1B
issuerid2	検索した交換内容の v2 の issuerid	16B
size2	検索した交換内容の v2 の size	2B
v2	検索した交換内容の v2 の内容	(size2) B

6.4.4 ExgStatusList

ICC_XがAP_Xに対して，交換途中の ThreadID のリストを通知するメッセージ.
本メッセージは RequestExgStatusList メッセージに対応する出力メッセージとして生成される.
ICC_Xは，スレッド ID である ExhThreadID と遷移状態 state の組のリストである ExgStatusList を DATA としてメッセージを生成する.

Parameters：

DATA 詳細

ThreadIDList	スレッド ID リスト	
ThreadIDNum	交換内容の個数	2B
ThreadIDInfo	交換内容のリスト	
state	状態管理パラメータ	1B
ExgThreadID	交換正常処理中のスレッド ID	20B

Appendix. APDU コマンド

本章では，IC カードに対するメッセージの送信元・宛先の指定が不要，または指定できない命令について，APDU コマンドとして規定する．IC カードは本章で規定する APDU コマンドを受理して処理を行い，APDU レスポンスフォーマットで結果を出力する．なお，APDU コマンドを受理できるのは，ISO7816-4 に準拠した IC カードのみである．

A.1 ReqIccID

IC カードの利用者は，本コマンドを用いて IC カードの eTRON ID の読み出しを行う．IC カードは，eTRON ID を含む APDU レスポンスを出力する．

ReqIccID コマンドフォーマット

	意味	データサイズ	規定値	備考
CLA	命令クラス	1B	80h	ISO/IEC7816-4 非準拠 SeM※無し
INS	命令コード	1B	F4h	ReqIccID コマンド
P1	命令パラメータ 1	1B	00h	
P2	命令パラメータ 2	1B	00h	
Lc	コマンドに対するレスポンスの予想される DATA 部長	3B	000000h	固定値

※SeM：セキュアメッセージング

ReqIccID レスポンスフォーマット

記号	意味	データサイズ	規定値	備考
DATA	レスポンス DATA 部	16B	-	DATA 詳細参照
SW1	コマンド処理ステータス	1B	**h	規定値：SW1/SW2 参照
SW2	コマンド処理修飾子	1B	**h	規定値：SW1/SW2 参照

DATA 詳細

データ	内容	データ長
eTRON ID	ICC の eTRON ID (domain(12) || port(4))	16

SW1-SW2 一覧

内容	値
正常終了	9000h
LEN エラー	6700h
実行条件を満足しない	6985h
P1-P2 エラー	6A86h
INS エラー	6D00h
CLA エラー	6E00h

A.2 Unlock

IC カードの利用者は，本コマンドを用いて IC カードへの書き込みを制御する情報 ICCState の LOCKED 状態を解除し，UNLOCKED 状態に遷移させる．

IC カードは，UNLOCK 用 PIN を認証すると，カードの状態を LOCK 状態から UNLOCKED 状態に遷移して，APDU レスポンスを出力する．本コマンドを用いて UNLOCKED 状態に遷移させた場合、BackUpInfo メッセージにより IC カードから出力していたファイル情報を，RestoreCard メッセージで書き戻す事はできなくなる．

Unlock コマンドフォーマット

記号	意味	データサイズ	規定値	備考
CLA	命令クラス	1B	80h	ISO/IEC7816-4 非準拠 SeM※無し
INS	命令コード	1B	F6h	Unlock コマンド
P1	命令パラメータ 1	1B	00h	
P2	命令パラメータ 2	1B	00h	

※ SeM：セキュアメッセージング

Unlock レスポンスフォーマット

記号	意味	データサイズ	規定値	備考
SW1	コマンド処理ステータス	1B	**h	規定値：SW1/SW2 参照
SW2	コマンド処理修飾子	1B	**h	規定値：SW1/SW2 参照

SW1-SW2 一覧

内容	値
正常終了	9000h
LEN エラー	6700h
メモリの書き込みに失敗した	6581h
実行条件を満足しない	6985h
P1-P2 エラー	6A86h
INS エラー	6D00h
CLA エラー	6E00h

参考文献

［THIF03］寺田，花舘，井口，藤村．公平な権利価値流通のための楽観的な交換プロトコル，CSS2003，Sep. 2003.

